



SANS TOP-20

Versione 7.0 del 15 Novembre 2006

Copyright © 2006, SANS Institute

La Top-20 degli obiettivi di attacco alla sicurezza in Internet

(Aggiornamento 2006)

Introduzione	2
W1. Internet Explorer	2
W2. Librerie di Windows	5
W3. Microsoft Office.....	7
W4. Servizi Windows	9
W5 Configurazioni deboli di Windows.....	10
M1. Mac OS X.....	12
U1. Configurazioni deboli di UNIX	13
C1 Applicazioni Web	15
C2. Database Software.....	17
C3. Applicazioni per la condivisione P2P	21
C4. Instant Messaging	24
C5. Lettori multimediali	26
C6. Server DNS	29
C7. Software di Backup	31
C8. Directory Server, sistemi di monitoraggio e per la gestione della sicurezza.....	32
N1 Server e telefoni VoIP	34
N2. Debolezze diffuse nella configurazione dei dispositivi di rete	35
H1. Diritti eccessivi dell'utente e dispositivi non autorizzati.....	37
H2. Utenti (Phishing e Spear Phishing)	38
Z1: Sezione speciale: Attacchi Zero Day e strategie di prevenzione	40

Introduzione

Sei anni or sono, il SANS Institute e il National Infrastructure Protection Center (NIPC) presso l'FBI rilasciarono un documento che riassumeva le Dieci vulnerabilità più critiche per la sicurezza in Internet. Migliaia di organizzazioni hanno riposto la loro fiducia in quella lista e sulle liste allargate alle Top 20 che sono seguite negli anni successivi, concentrando quindi i loro sforzi nel correggere in via prioritaria i buchi più pericolosi. I servizi vulnerabili che hanno portato alla diffusione di worm come Blaster, Slammer e Code Red erano tutti già compresi nelle liste SANS Top20.

La lista SANS Top-20 2006 non è "cumulativa." Abbiamo inserito solo vulnerabilità critiche che risalgono all'ultimo anno circa. Se quindi non avete corretto e aggiornato i vostri sistemi da molto tempo è altamente raccomandabile che sistemiate anche le vulnerabilità indicate nella Top-20 2005, oltre che quelle presenti nella lista 2006. Alla fine di questo documento troverete una breve serie di SANS Top-20 FAQ (domande frequenti) che rispondono ai dubbi che potreste avere riguardo il progetto in questione e il sistema con cui la lista viene creata..

La SANS Top-20 2006 è una lista largamente condivisa delle vulnerabilità che richiedono una riparazione immediata. Si tratta del risultato di un processo che coinvolge dozzine dei più importanti esperti di sicurezza mondiali che provengono dalle agenzie governative più impegnate nella sicurezza di Gran Bretagna, Stati Uniti e Singapore, dalle principali case produttrici di software e le più importanti società di consulenza, dai maggiori programmi universitari di ricerca nel campo della sicurezza, dall'Internet Storm Center e da molte altre organizzazioni di utenti. Potete trovare una lista dei partecipanti alla fine del documento.

La lista SANS Top-20 è un documento in continuo aggiornamento. Contiene istruzioni dettagliate e riferimenti a informazioni supplementari utili per risolvere i problemi di sicurezza. Quando vengono scoperte nuove minacce critiche o sono identificati metodi di protezione più aggiornati o più efficaci, vengono aggiornati la lista delle vulnerabilità e le istruzioni per correggerle; in questo processo il vostro contributo è sempre gradito.

Questo documento si basa sul consenso di una intera comunità: la vostra esperienza nel combattere gli attacchi e nell'eliminare le vulnerabilità può aiutare quelli che verranno dopo di voi. Inviare i vostri suggerimenti via e-mail all'indirizzo top20@sans.org

W1. Internet Explorer

W1.1 Descrizione

Microsoft Internet Explorer è il browser per la navigazione del web più diffuso e viene installato per default su tutti i sistemi Windows. Le versioni più datate o non aggiornate di Internet Explorer contengono svariate vulnerabilità che possono portare a problemi di memoria, spoofing (siti web ingannevoli) e all'esecuzione incontrollata di script potenzialmente dannosi. I problemi più gravi sono quelli che portano all'esecuzione di codice in modalità remota senza alcun intervento dell'utente mentre si visita una pagina web o si legge un messaggio email. Il codice per sfruttare molte delle vulnerabilità critiche di Internet Explorer è disponibile pubblicamente. Come se non bastasse, Internet Explorer viene utilizzato come leva per sfruttare le vulnerabilità presenti in altri componenti fondamentali di Windows come l'Help HTML e il Graphics Rendering Engine. Ci si server di Internet Explorer, inoltre, per sfruttare i problemi presenti nei controlli ActiveX installati da Microsoft o da altri produttori di software.

Queste vulnerabilità sono state largamente utilizzate per installare spyware, adware ed altro software dannoso sui sistemi degli utenti di tutto il mondo. I problemi di spoofing sono la base per condurre gli attacchi di phishing (la duplicazione di pagine web atta carpire all'utente informazioni personali, finanziarie o semplicemente le sue password). Sono molti anche i casi di vulnerabilità cosiddette zero-days per le quali la patch (la rettifica della parte del software che consente di risolvere il problema) non era disponibile al momento in cui la vulnerabilità è stata resa pubblica. Ad esempio la vulnerabilità VML **zero-day** risolta dalla patch Microsoft MS06-055 fu sfruttata per lungo tempo da siti web malevoli prima che il rimedio fosse disponibile.

Nel corso dell'anno appena trascorso, Microsoft ha rilasciato diversi aggiornamenti per Internet Explorer.

- La vulnerabilità in Vector Markup Language può consentire l'esecuzione di codice in modalità remota ([MS06-055](#))
- Aggiornamento cumulativo per la protezione di Internet Explorer ([MS06-042](#))

SANS Top

La versione italiana è curata da Data Security - www.datasecurity.it

- Una vulnerabilità in Microsoft JScript può consentire l'esecuzione di codice in modalità remota ([MS06-023](#))
- Aggiornamento cumulativo per la protezione di Internet Explorer ([MS06-021](#))
- Aggiornamento cumulativo per la protezione di Internet Explorer ([MS06-013](#))
- Aggiornamento cumulativo per la protezione di Internet Explorer ([MS06-004](#))
- Aggiornamento cumulativo per la protezione di Internet Explorer ([MS05-054](#))

Si noti che il più recente aggiornamento cumulativo per la protezione di Internet Explorer comprende tutti gli aggiornanti cumulativi precedenti.

Anche la patch [MS06-051](#) è importante per Internet Explorer perché, sebbene risolva una vulnerabilità del kernel di Windows, senza questa patch è presente in Internet Explorer una vulnerabilità di denial-of-service (interruzione del servizio) che può essere verosimilmente sfruttata per l'esecuzione di codice non autorizzato.

W1.2 Sistemi operativi interessati

Sono potenzialmente vulnerabili Internet Explorer 5.x e 6.x operanti su Windows 98/ME/SE, Windows NT Workstation e Server, Windows 2000 Workstation e Server, Windows XP Home e Professional, Windows 2003.

W1.3 Riferimenti CVE

[CVE-2005-2831](#), [CVE-2006-0020](#), [CVE-2006-1185](#), [CVE-2006-1186](#), [CVE-2006-1188](#), [CVE-2006-1189](#), [CVE-2006-1245](#), [CVE-2006-1303](#), [CVE-2006-1313](#), [CVE-2006-1359](#), [CVE-2006-1388](#), [CVE-2006-2218](#), [CVE-2006-2382](#), [CVE-2006-2383](#), [CVE-2006-3450](#), [CVE-2006-3451](#), [CVE-2006-3637](#), [CVE-2006-3638](#), [CVE-2006-3639](#), [CVE-2006-3873](#), [CVE-2006-4868](#)

W1.4 Come stabilire se si è a rischio

Utilizzate un qualsiasi vulnerability scanner per verificare se il vostro sistema è protetto rispetto ai problemi elencati. Prendete anche in considerazione l'uso di sistemi per la valutazione dello stato degli aggiornamenti dei vostri sistemi quali Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) o Systems Management Server ([SMS](#)).

W1.5 Come proteggersi da queste vulnerabilità

- Se utilizzate Internet Explorer sui vostri sistemi, il modo migliore per rimanere sicuri è quello di aggiornarli a Windows XP Service Pack 2. I miglioramenti nella sicurezza del sistema operativo e il Windows Firewall contribuiranno a ridurre i rischi. A coloro che non possono passare a Windows XP con Service Pack 2 è vivamente raccomandato l'utilizzo di un diverso browser.
- Si raccomanda anche il passaggio alla versione 7 di Internet Explorer, che fornisce una sicurezza maggiore rispetto alle versioni precedenti. L'ultima versione di Internet Explorer, IE7, viene distribuita da Microsoft come aggiornamento critico ([KB926874](#))
- Mantenete i sistemi aggiornati con le patch e i service pack più recenti. Quando possibile, abilitate l'opzione [Aggiornamenti automatici](#) su tutti i sistemi.
- Per ridurre l'esposizione agli attacchi zero day, prestate attenzione ai [Bollettini sulla sicurezza](#) Microsoft e mettete in atto i suggerimenti per ridurre il pericolo prima che la patch sia disponibile.
- Per prevenire la possibilità di sfruttare le vulnerabilità che consentono l'esecuzione di codice in modalità remota a livello di Amministratore, si possono usare strumenti quali Microsoft [DropMyRights](#) eseguire Internet Explorer con "privilegi minimi".
- Evitate che componenti ActiveX vulnerabili siano operativi attraverso Internet Explorer con il meccanismo "killbit" (Interruzione dell'esecuzione di un controllo ActiveX in Internet Explorer)
- Molti programmi spyware vengono installati quali Assistente del Browser (Browser Helper Object). Un Browser Helper Object o BHO è un piccolo programma che viene automaticamente eseguito ogni volta che si avvia Internet Explorer e ne aggiunge alcune funzionalità. I Browser Helper Object possono essere individuati utilizzando uno scanner Antispyware.

- Utilizzate sistemi di Intrusion Prevention/Detection e software Anti-virus, Anti-Spyware e Malware per bloccare il codice di script HTML dannosi.
- I sistemi Windows 98/ME/NT non sono più supportati per quel che riguarda gli aggiornamenti. Coloro che ancora li usano dovrebbero valutare la possibilità di passare a Windows XP.
- Prendete in considerazione l'utilizzo di browser diversi, che non supportino la tecnologia ActiveX come, . Ad esempio, Mozilla Firefox.

W1.6 Come rendere sicuro Internet Explorer

Per configurare le impostazioni di sicurezza di Internet Explorer:

- Scegliere *Opzioni Internet* dal menu *Strumenti*.
- Scegliere l'opzione *Protezione* e quindi impostare *Livello personalizzato* nell'area *Internet*.

La maggior parte delle vulnerabilità di IE vengono sfruttate attraverso Active Scripting o i Controlli ActiveX.

- Nella sezione *Esecuzione script*, scegliete *Disattiva* per la voce "*Consenti operazioni di copia tramite script*" per evitare che sia possibile vedere i contenuti dei vostri appunti (clipboard). Nota: Disabilitando Active Scripting è possibile che alcuni siti web non funzionino più correttamente.

I Controlli ActiveX sono meno conosciuti, ma sono potenzialmente molto più pericolosi in quanto permettono un maggiore accesso al sistema

- Scegliete *Disattiva* per la voce "*Scarica controlli ActiveX con firma elettronica*". Scegliete *Disattiva* anche per la voce "*Scarica controlli ActiveX senza firma elettronica*" e "*Inizializza e esegui script controlli ActiveX non contrassegnati come sicuri*".

Gli applet Java hanno di solito potenzialità anche maggiori rispetto agli script.

- Sotto *Microsoft VM*, scegliete *Protezione Alta* per le *Autorizzazioni Java*, in modo da mantenere sotto controllo gli applet Java ed evitare un accesso con privilegi al vostro sistema.
- Sotto *Varie*, selezionate *Disattiva* alla voce "*Accesso all'origine dati a livello di dominio*", per evitare gli attacchi Cross-site scripting.

Controllate anche non vi sia alcun sito sospetto nell'area *Siti attendibili* e nell'*Intranet Locale*, in quanto per queste aree le impostazioni di sicurezza sono inferiori rispetto alle altre.

W1.7 Riferimenti

Aggiornamenti per la sicurezza di Internet Explorer

- <http://www.microsoft.com/italy/technet/security/bulletin/ms06-055.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=38#widely1>
- <http://www.microsoft.com/italy/technet/security/bulletin/ms06-042.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=32#widely2>
- <http://www.microsoft.com/italy/technet/security/bulletin/ms06-023.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=24#widely5>
- <http://www.microsoft.com/italy/technet/security/bulletin/ms06-021.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=24#widely1>
- <http://www.microsoft.com/italy/technet/security/bulletin/ms06-013.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=12#widely1>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=11#widely4>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=12#widely1>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=15#widely1>
- <http://www.microsoft.com/italy/technet/security/bulletin/ms06-004.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=5&i=6#widely1>

- <http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely2>
- <http://www.microsoft.com/italy/technet/security/bulletin/ms05-054.msp>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=50#widely1>

Informazioni sulla sicurezza dei Browser Web US-CERT

- http://www.us-cert.gov/reading_room/securing_browser/browser_security.html

W2. Librerie di Windows

W2.1 Descrizione

Le librerie di Windows sono moduli che contengono funzioni e dati che possono essere utilizzati da diversi componenti quali le applicazioni di Windows. Le applicazioni di Windows si avvalgono spesso di un numero molto elevato di queste librerie, che spesso sono archiviate come librerie di collegamento dinamico (DLL), per eseguire le proprie funzioni. Queste librerie di solito sono file con estensione DLL o OCX (per le librerie che contengono i controlli ActiveX).

Le DLL permettono di rendere modulari le applicazioni in modo che le loro funzionalità possano essere facilmente aggiornate e riutilizzate. Le DLL aiutano anche a ridurre i picchi di memoria quando molte applicazioni utilizzano contemporaneamente la stessa funzionalità. Queste librerie vengono utilizzate per molti compiti comuni come il parsing HTML, la decodifica del formato delle immagini o dei protocolli. Esse vengono utilizzate sia dalle applicazioni locali, sia da quelle accessibili in modalità remota. Di conseguenza una vulnerabilità critica in una libreria ha effetto su tutta una serie di applicazioni di Windows e di altri produttori di software che fanno affidamento sulla libreria stessa e quindi spesso la vulnerabilità diventa sfruttabile mediante strade diverse. Ad esempio, i bachi presenti nelle librerie che eseguono l'elaborazione elettronica delle immagini possono essere sfruttati tramite Internet Explorer, tramite Office o tramite i visualizzatori di immagini. In molti casi, inoltre, le librerie sono utilizzate da tutti i tipi e le versioni di sistemi operativi Windows, il che ovviamente aumenta il numero di sistemi che possono essere obiettivo di ciascun attacco.

Durante l'anno appena trascorso è stato rilevato che diverse librerie sono soggette a vulnerabilità critiche. In diversi casi il codice per sfruttarle è stato scoperto prima che la patch fosse disponibile (**zero-day**).

Nel Dicembre 2005 è stata annunciata una vulnerabilità (CVE-2005-4560) del motore di rendering della grafica (Graphics Rendering Engine): quando questo era chiamato a gestire delle immagini Windows Metafile (WMF) costruite in modo particolare, poteva fare in modo che venisse eseguito del codice non autorizzato. Ci si accorse presto che molti exploit dannosi e diversi malware (codici nocivi) si propagarono largamente attraverso Internet subito dopo la scoperta della vulnerabilità. Siccome tale vulnerabilità può essere sfruttata tramite la mera visualizzazione di un file WMF confezionato ad arte (presente, ad esempio, in un sito Web o come allegato in un messaggio di posta elettronica), il problema ebbe effetto su diverse applicazioni. Risultarono colpite da questo exploit WMF zero-day perfino alcune versioni di Lotus Notes. Non è stata disponibile alcuna patch fino all'inizio di gennaio 2006. I dettagli su questa vulnerabilità e sui relative exploit sono reperibili all'indirizzo: <http://isc.sans.org/diary.php?storyid=993>

Siccome le vulnerabilità nelle librerie Windows possono essere sfruttate da cali diversi, in molti casi un aggressore remoto dovrà semplicemente persuadere un utente ad accedere ad un sito realizzato ad hoc, a una immagine, un'icona o un file del cursore per avere la possibilità di eseguire codice non autorizzato sul sistema dell'utente, con i privilegi in uso dall'utente stesso.

Le vulnerabilità critiche che hanno colpito le librerie importanti nell'anno appena trascorso comprendono:

- Una vulnerabilità in Esplora risorse può consentire un'esecuzione in modalità remota (**MS06-057, MS06-015**).
- Alcune vulnerabilità nella libreria di oggetti Collegamento ipertestuale di Microsoft Windows possono consentire l'esecuzione di codice in modalità remota (**MS06-050**)
- Una vulnerabilità nella Guida HTML può consentire l'esecuzione di codice in modalità remota (**MS06-046**)
- Una vulnerabilità in Microsoft Windows può consentire l'esecuzione di codice in modalità remota (**MS06-043**)

- Una vulnerabilità del motore di rendering della grafica può consentire l'esecuzione di codice in modalità remota ([MS06-026](#), [MS06-001](#))
- Una vulnerabilità nei caratteri Web incorporati può consentire l'esecuzione di codice in modalità remota ([MS06-002](#))

W2.2. Sistemi operativi interessati

Windows NT, Windows 2000, Windows XP, Windows 2003

W2.3. Riferimenti CVE

[CVE-2005-4560](#), [CVE-2006-0010](#), [CVE-2006-0012](#), [CVE-2006-2376](#), [CVE-2006-2766](#), [CVE-2006-3086](#), [CVE-2006-3357](#), [CVE-2006-3438](#), [CVE-2006-3730](#), [CVE-2006-4868](#)

W2.4. Come stabilire se si è a rischio

- Utilizzate un qualsiasi vulnerability scanner per verificare se il vostro sistema è protetto rispetto ai problemi elencati. Prendete anche in considerazione l'uso di sistemi per la valutazione dello stato degli aggiornamenti dei vostri sistemi quali Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) o Systems Management Server ([SMS](#)).
- Potete verificare la presenza della patch corrispondente anche controllando la chiave del registro citata nella sezione Controllo delle chiavi del Registro di sistema presente nel relativo Bollettino sulla sicurezza. È opportuno, inoltre, controllare che le versioni aggiornate dei file citati nel bollettino siano installate sul sistema.

W2.5. Come proteggersi da queste vulnerabilità

- Controllate che i vostri sistemi Windows abbiano installate i più recenti aggiornamenti di sicurezza.
- Bloccate a livello di perimetro della vostra rete le porte tcp dalla 135 alla 139, la 445/tcp e le altre porte utilizzate dai sistemi Windows. Questa operazione impedisce attacchi da remoto che sfruttino le vulnerabilità tramite file system condivisi.
- Utilizzate il sistema di Filtro TCP/IP disponibile in Windows 2000 e XP, il Windows Firewall dei sistemi Windows XP o qualche altro personal firewall per bloccare il traffico in entrata sulle porte in questione. È importante che il firewall sia configurato correttamente perché possa efficacemente fermare gli attacchi provenienti dall'esterno.
- I sistemi di Intrusion Prevention/Detection e i software Anti-virus e Anti-Malware sono estremamente utili per rafforzare la protezione dal codice dannoso e dagli exploit che sfruttano questo tipo di vulnerabilità.
- Se utilizzate applicazioni di terze parti su piattaforme Windows 2000/XP personalizzate, controllate che sia applicata una patch appropriata per ciascun fornitore.
- Seguite il principio dei "Privilegi minimi " per limitare la possibilità che worm e Trojan usino i vostri sistemi come punto di appoggio. Maggiori dettagli su come limitare l'accesso a determinate chiavi di registro, a file eseguibili e a particolari cartelle sono disponibili nelle guide NSA, reperibili all'indirizzo <http://www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1>.
- Applicate le procedure per rendere i sistemi più sicuri (ad esempio quelli fornite da [CISecurity](#)) per rendere i sistemi più resistenti ad attacchi locali e remoti.
- Mantenetevi aggiornati sulle novità e gli aggiornamenti sulla sicurezza Microsoft (<http://www.microsoft.com/italy/security/default.mspx>).
- Siccome le vie per apportare questi tipi di attacchi sono molto numerose, siate particolarmente guardinghi quando ricevete allegati di posta elettronica non richiesti e quando navigate su siti Web poco conosciuti. Non seguite i link non richiesti che vi arrivano tramite email, nei messaggi dei sistemi di instant messaging, nei forum o dai canali internet relay chat (IRC).
- Windows NT non viene più supportato. Bisogna passare a Windows XP/2003.

W2.6. Riferimenti

Una vulnerabilità in Esplora risorse può consentire l'esecuzione di codice in modalità remota

<http://www.microsoft.com/italy/technet/security/bulletin/ms06-057.msp>

<http://www.microsoft.com/italy/technet/security/bulletin/ms06-015.msp>

La vulnerabilità in Vector Markup Language può consentire l'esecuzione di codice in modalità remota

<http://www.microsoft.com/italy/technet/security/bulletin/ms06-055.msp>

Alcune vulnerabilità nella libreria di oggetti Collegamento ipertestuale di Microsoft Windows possono consentire l'esecuzione di codice in modalità remota

<http://www.microsoft.com/italy/technet/security/bulletin/ms06-050.msp>

<http://www.microsoft.com/italy/technet/security/bulletin/ms05-015.msp>

Una vulnerabilità nella Guida HTML può consentire l'esecuzione di codice in modalità remota

<http://www.microsoft.com/italy/technet/security/bulletin/ms06-046.msp>

<http://www.microsoft.com/italy/technet/security/bulletin/ms05-026.msp>

<http://www.microsoft.com/italy/technet/security/bulletin/ms05-001.msp>

Una vulnerabilità in Microsoft Windows può consentire l'esecuzione di codice in modalità remota

<http://www.microsoft.com/italy/technet/security/bulletin/ms06-043.msp>

Una vulnerabilità del motore di rendering della grafica può consentire l'esecuzione di codice in modalità remota

<http://www.microsoft.com/italy/technet/security/bulletin/ms06-026.msp>

<http://www.microsoft.com/italy/technet/security/bulletin/ms06-001.msp>

<http://www.microsoft.com/italy/technet/security/bulletin/ms05-053.msp>

Una vulnerabilità nei caratteri Web incorporati può consentire l'esecuzione di codice in modalità remota

<http://www.microsoft.com/italy/technet/security/bulletin/ms06-002.msp>

W3. Microsoft Office

W3.1 Descrizione

Microsoft Office è la suite per la posta elettronica e la produttività individuale più utilizzata al mondo.

Comprende applicazioni quali Outlook, Word, PowerPoint, Excel, Visio, FrontPage e Access. Le vulnerabilità presenti in questi prodotti vengono sfruttate tramite le seguenti direttrici d'attacco::

- L'aggressore spedisce il documento Office dannoso in un messaggio email. I virus di solito utilizzano questa strada.
- L'aggressore inserisce il documento su un web server o una cartella condivisa e istiga l'utente ad accedere alla pagina Web o alla cartella condivisa. Si noti che Internet Explorer apre automaticamente i documenti Office, per cui la sola visita alla pagina Web o alla cartella è sufficiente per approfittare della vulnerabilità.
- L'aggressore opera con un server di news o dirotta il flusso di un feed RSS che spedisce documenti dannosi ai client email.

Nell'anno appena passato sono state rilevati numerosi problemi critici per quanto riguarda le applicazioni MS Office. Si aggiunga il fatto che alcune di queste ([CVE-2006-5296](#), [CVE-2006-4694](#), [CVE-2006-4534](#), [CVE-2006-3649](#), [CVE-2006-3590](#), [CVE-2006-3059](#), [CVE2006-2492](#), [CVE-2006-1540](#), [CVE-2006-1301](#)) sono state utilizzate nella fase **zero-day**, quando non era ancora disponibile alcuna correzione da parte del produttore, fatto questo che rappresenta una tendenza in continua crescita.. Il codice per l'Exploit e i dettagli tecnici di alcune di queste vulnerabilità sono pubblicamente disponibili.

I problemi critici rilevati lo scorso anno in Office e Outlook Express sono:

- Vulnerabilità di PowerPoint che possono consentire l'esecuzione di codice in modalità remota ([CVE-2006-5296](#))
- Vulnerabilità legata allo stack non valido in Microsoft Word ([MS06-060](#))
- Vulnerabilità di mso.dll per Office e Power Point ([MS06-062](#), [MS06-048](#))
- Vulnerabilità in Microsoft Excel possono consentire l'esecuzione di codice in modalità remota ([MS06-059](#))

- Vulnerabilità legata al record di dati non valido in PowerPoint ([MS06-058](#))
- Vulnerabilità di Visual Basic per Visio, Works e Projects ([MS06-047](#))
- Vulnerabilità legata all'analisi delle stringhe non valide in Microsoft Office ([MS06-038](#))
- Vulnerabilità legata al record SELECTION non valido in Microsoft Excel ([MS06-037](#))
- Vulnerabilità legata al puntatore a oggetto non valido in Microsoft Word ([MS06-027](#))
- Vulnerabilità legata alla decodifica TNEF in Outlook e Exchange ([MS06-003](#))

W3.2 Sistemi operativi interessati

Windows 9x, Windows 2000, Windows XP, Windows 2003 sono tutti vulnerabili in conseguenza della versione di Office installata.

W3.3 Riferimenti CVE

[CVE-2006-5296](#), [CVE-2006-4694](#), [CVE-2006-4534](#), [CVE-2006-3649](#), [CVE-2006-3590](#), [CVE-2006-3059](#), [CVE-2006-2492](#), [CVE-2006-1540](#), [CVE-2006-1301](#), [CVE-2006-0002](#)

W3.4 Come stabilire se si è a rischio

Sono vulnerabili le installazioni di MS Office che operano senza le patch citate nei Bollettini Microsoft elencati nei record NVD citati qui sopra. Utilizzate un qualsiasi vulnerability scanner per verificare se il vostro sistema è protetto rispetto ai problemi elencati. Prendete anche in considerazione l'uso di sistemi per la valutazione dello stato degli aggiornamenti dei vostri sistemi quali Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) o Systems Management Server ([SMS](#)).

W3.5 Come proteggersi dalle vulnerabilità di Microsoft Office

- Mantenete i sistemi aggiornati con le patch e i service pack più recenti. Se possibile, abilitate gli Aggiornamenti automatici su tutti i sistemi.
- Disabilitate la funzione di Internet Explorer che apre automaticamente i documenti Office.
- Configurate Outlook e Outlook Express con le impostazioni di protezione avanzate.
- Utilizzate sistemi di Intrusion Prevention/Detection e software Anti-virus e per la rilevazione di Malware per evitare che documenti e risposte del server dannose raggiungano gli utenti finali della vostra rete.
- Utilizzate sistemi di filtro dei contenuti web e delle email a livello di rete per evitare che documenti Office dannosi raggiungano i sistemi degli utenti finali.

W3.6 Riferimenti

Discussioni su vulnerabilità zero-day di Microsoft Office

<http://blogs.technet.com/msrc/archive/2006/10/12/poc-published-for-ms-office-2003-powerpoint.aspx>

<http://blogs.securiteam.com/?p=508>

http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-081616-2104-99

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FMDROPPER%2EBI&Vsect=T>

<http://blogs.securiteam.com/?p=451>

http://www.symantec.com/security_response/writeup.jsp?docid=2006-051911-0706-99

http://www.symantec.com/security_response/writeup.jsp?docid=2006-051914-5151-99

W4. Servizi Windows

W4.1 Descrizione

La famiglia dei sistemi operativi Windows supporta una larga gamma di servizi, procedure di rete e tecnologie. Molti di questi componenti sono implementati come SCP (Service Control Programs) (SCP) sotto il controllo del Service Control Manager – SCM (Strumenti di amministrazione – Servizi), che viene eseguito come Services.exe. Le vulnerabilità dei servizi che eseguono queste funzioni del sistema operativo sono una delle strade più battute per gli attacchi alla sicurezza.

Molti dei servizi del nucleo centrale di Windows forniscono punti di collegamento remoti ai componenti del client attraverso le Chiamate di procedura remota (Remote Procedure Calls - RPC). Questi sono esposti soprattutto attraverso le procedure accessibili tramite il protocollo CIFS (Common Internet File System), alcune porte TCP/UDP ben conosciute e in alcuni casi attraverso porte TCP/UDP più transitorie. Storicamente vi sono state numerose vulnerabilità nei servizi Windows che potevano essere sfruttate con utenti anonimi. Quando vengono sfruttate, queste vulnerabilità offrono all'aggressore gli stessi privilegi che ha presso l'host il servizio in quel momento attivo.

Le precedenti versioni dei sistemi operativi Windows, in particolare Windows NT e Windows 2000, abilitano per default molti di questi servizi per fare in modo che il sistema risulti già attivo in tutte le sue componenti senza bisogno di particolari configurazioni, ma tali servizi spesso non necessari e talvolta inutili per le esigenze di molti utenti aumentano significativamente la possibilità di subire degli attacchi.

Le vulnerabilità critiche nei Servizi Windows riportate lo scorso anno nei bollettini riguardano:

- Servizio Server ([MS06-040](#), [MS06-035](#))
- Servizio Routing e Accesso remoto ([MS06-025](#))
- Servizio Exchange ([MS06-019](#))

Esiste del codice per sfruttare queste vulnerabilità. Le vulnerabilità corrette con l'aggiornamenti [MS06-040](#) sono state utilizzate dai worm [W32.Dasher.G](#) e [W32.Spybot.AKNO](#).

W4.2 Sistemi operativi interessati

Sono potenzialmente vulnerabili Windows 2000 Workstation e Server, Windows XP Home e Professional, Windows 2003.

W4.3 Riferimenti CVE

[CVE-2006-0027](#), [CVE-2006-1314](#), [CVE-2006-2370](#), [CVE-2006-2371](#), [CVE-2006-3439](#)

W4.4 Come stabilire se si è a rischio

- Utilizzate un qualsiasi vulnerability scanner per verificare se il vostro sistema è protetto rispetto ai problemi elencati. Prendete anche in considerazione l'uso di sistemi per la valutazione dello stato degli aggiornamenti dei vostri sistemi quali Microsoft Windows Server Update Services ([WSUS](#)), Microsoft Baseline Security Analyzer ([MBSA](#)), [Windows Live Scanner](#) o Systems Management Server ([SMS](#)).
- Potete verificare la presenza della patch corrispondente anche controllando la chiave del registro citata nella sezione Controllo delle chiavi del Registro di sistema presente nel relativo Bollettino sulla sicurezza. È opportuno, inoltre, controllare che le versioni aggiornate dei file citati nel bollettino siano installate sul sistema.
- Per verificare se il vostro sistema sia vulnerabile a un problema presente in un servizio opzionale, dovete prima controllare se il servizio è avviato. Si può fare attraverso la console di amministrazione dei Servizi, che può essere lanciata al menu Servizi in Strumenti di Amministrazione.

W4.5 Come proteggersi dalle vulnerabilità dei Servizi Windows

- Mantenete i sistemi aggiornati con le patch e i service pack più recenti. Se possibile, abilitate gli Aggiornamenti automatici su tutti i sistemi.

- Utilizzate sistemi di Intrusion Prevention/Detection per prevenire/identificare attacchi che sfruttino queste vulnerabilità.
- In alcuni casi i rischi legati a queste vulnerabilità possono essere eliminati disabilitando il servizio corrispondente. Il servizio di Routing e Accesso remoto, ad esempio, può essere tranquillamente disabilitato nella maggior parte degli ambienti che utilizzano Windows 2000. Per fare ciò, avviate la console di gestione dei Servizi, trovate il servizio incriminato e selezionatelo con il tasto destro del mouse. Richiamate la voce Proprietà nel menu a tendina e selezionate *Disabilitato* nella casella *Tipo di avvio*.
- Disabilitate la funzione di Internet Explorer che apre automaticamente i documenti Office.
- Configurate Outlook e Outlook Express con le impostazioni di protezione avanzate.
- Utilizzate sistemi di filtro dei contenuti web e delle email a livello di rete per evitare che documenti Office dannosi raggiungano i sistemi degli utenti finali.
- In alcuni casi è possibile usare lo stratagemma di impedire l'accesso a sessioni nulle verso la interfaccia vulnerabile. È buona norma rivedere le vostre impostazioni correnti di RestrictAnonymous e impostarle nella forma più limitativa possibile in base al vostro ambiente di lavoro <http://www.securityfocus.com/infocus/1352>
- Molte di queste vulnerabilità si trovano sui collegamenti permessi da CIFS: bloccare le porte tcp 139 e 445 a livello perimetrale è essenziale per prevenire attacchi da remoto. È buona norma anche bloccare le chiamate RPC in entrata provenienti da Internet verso porte superiori alla 1024 per bloccare altre vulnerabilità basate su che utilizzano i firewall.
- XP SP2 e Windows 2003 SP1 e R2 presentano diversi miglioramenti in termini di sicurezza, incluso il Windows firewall e il Security Configuration Wizard (solo per Windows 2003 SP1 e R2). È quindi assolutamente raccomandabile aggiornare i vostri sistemi con questi service pack, abilitare il Windows firewall e ridurre la possibilità di attacchi con il Security Configuration Wizard.

W4.6 Riferimenti

Introduzione ai pericoli e alle contromisure: Impostazioni di sicurezza per Windows Server 2003 e Windows XP

<http://www.microsoft.com/italy/technet/security/topics/serversecurity/tcg/tcgch01n.mspix>

Guida per la protezione di Windows XP

<http://www.microsoft.com/italy/technet/security/prodtech/windowsxp/secwinxp/default.mspix>

Guida per la protezione di Windows Server 2003

<http://www.microsoft.com/italy/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspix>

Informazioni su Windows Firewall

http://www.microsoft.com/italy/windows/products/windowsxp/winxp/using/security/internet/sp2_wfintro.mspix

Informazioni sulla Configurazione guidata impostazioni di sicurezza

<https://www.microsoft.com/technet/prodtechnol/windowsserver2003/it/library/ServerHelp/eeb7c8c2-3579-47cc-a126-6519321098e6.mspix?mfr=true>

Utilizzare gli elenchi di filtri IP IPSec in Windows 2000

<http://support.microsoft.com/kb/313190>

Blocco di specifici protocolli di rete e porte utilizzando IPSec

<http://support.microsoft.com/kb/813878>

Configurazione della funzionalità Filtro TCP/IP in Windows 2000

<http://support.microsoft.com/kb/309798>

W5 Configurazioni deboli di Windows

W5.1 Descrizione

1. Problemi di configurazione per le password degli utenti

La debolezza nella configurazione delle password hanno assunto negli ultimi anni una importanza sempre maggiore a causa del proliferare di worm, bot e altri malware che hanno aumentato la loro capacità di propagarsi attraverso l'abuso di password inadeguate. L'applicazione di vincoli per rendere complesse le password è uno dei problemi più antichi che si presentano a coloro che amministrano la sicurezza IT, eppure continua ad affliggere le aziende di tutto il mondo. Questi punti deboli possono riscontrarsi sia a livello di Active Directory, sia a livello locale ed entrambi possono essere sfruttati efficacemente da parte di codici maligni o da minacce interne. Si aggiunga che con l'avanzare dell'autenticazione centralizzata multi-piattaforma la minaccia alle credenziali di Windows può spesso portare a mettere in pericolo la sicurezza di credenziali di altri sistemi (es. UNIX e RACF/ACF2/Top Secret). Anche se sono state adottate password complesse nella grande maggioranza degli account, una sola password debole può portare a mettere a rischio una grande percentuale di account.

2. Password degli account dei Servizi

In Windows, gli account dei Servizi non di sistema hanno bisogno di password. Purtroppo è ancora una pratica molto comune l'utilizzo di password corte e stampabili per questi servizi. Questa prassi diventa particolarmente pericolosa in quanto spesso queste credenziali sono utilizzate su diverse macchine, hanno privilegi piuttosto elevate e vengono modificate molto raramente.

3. Log-on nulli

Le credenziali nulle sono state a lungo un problema negli ambienti dei domini Windows. Fin dalla nascita dell'architettura di dominio con Windows NT, le sessioni nulle hanno permesso ad utenti anonimi di elencare i sistemi, le condivisioni e gli account utente. Windows 2000 ha introdotto due livelli di controllo sull'accesso anonimo, ma questo controllo era disabilitato nelle impostazioni di default. Con l'avvento di Windows 2003, Microsoft ha aggiunto una serie di controlli sull'accesso anonimo ed abilitato per default una serie di restrizioni. Rimane il problema di sistemi meno aggiornati che molti sono ancora costretti a conservare per la compatibilità delle proprie applicazioni, i quali continuano a supportare le connessioni anonime.

W5.2 Come proteggersi dai problemi di configurazione

Password deboli:

- Implementate una rigida password policy per tutti gli utenti del dominio. Questa policy deve comprendere i criteri di complessità e la scadenza della password. Prendete in considerazione l'uso di strumenti di terze parti per la gestione della password degli account locali per verificare l'unicità delle password.
- Evitate che Windows archivi l'hash LM in Active Directory o nel database SAM seguendo le istruzioni fornite da Microsoft.
- Adottate una politica di controllo periodico delle password presenti in azienda. Questa verifica dovrebbe comprendere l'uso di strumenti automatizzati quali THC Hydra, LophtCrack e John the Ripper per controllare se vi siano password vuote, comuni o molto semplici. La verifica dovrebbe essere compiuta su tutte le piattaforme in uso e non limitarsi alle password di Active Directory.

Log-on nulli:

- Limitate l'accesso anonimo ai sistemi nel dominio. Consultate la sezione "Riferimenti" per i dettagli sull'impatto delle restrizioni delle sessioni nulle e le impostazioni possibili nei diversi scenari.

W5.3 Riferimenti

Guida alla pianificazione della protezione degli account amministrativi

<http://www.microsoft.com/italy/technet/security/topics/serversecurity/administratoraccounts/default.mspx>

Guide per la sicurezza di Windows

<http://www.microsoft.com/italy/technet/security/prodtech/windowsxp/secwinxp/default.mspx>

<http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0A0201F639A56&DisplayLang=en>

Come impedire a Windows di archiviare un hash di LAN Manager per la password in Active Directory e nei database SAM

<http://support.microsoft.com/kb/299656>

MSRPC NULL sessions -exploitation and protection

http://www.hsc.fr/ressources/presentations/null_sessions/null_sessions_explained.html

Restricting Anonymous Access

<http://technet2.microsoft.com/WindowsServer/en/library/2c82586e-bd58-42b7-9976228a23721e351033.msp?mfr=true>

Possibili incompatibilità tra client, servizi e programmi quando si modificano le impostazioni di protezione e le assegnazioni dei diritti utente

<http://support.microsoft.com/kb/823659>

Indicazioni di supporto alla configurazione della protezione

<http://support.microsoft.com/kb/885409>

M1. Mac OS X

M1.1 Descrizione

Mac OS X è il sistema operativo della Apple basato su BSD destinato alla propria linea di PowerPC e ai computer basati su Intel.

Per maggiori informazioni su Mac OS X, potete consultare l'indirizzo: <http://www.apple.com/macosex>

Mac OS X è costituito da numerosi componenti differenti. Ciascuno di questi componenti può potenzialmente avere dei problemi di sicurezza. La maggior parte delle vulnerabilità critiche scoperte nell'anno appena trascorso rientrano in sei diverse categorie:

- *Safari* – Il web browser Safari di Apple è il browser di default nelle versioni recenti di Mac OS X. Le vulnerabilità presenti in questa applicazione possono potenzialmente risolversi nel controllo completo del browser di un utente o della sessione di login.
- *ImageIO* – è il motore dell'ambiente applicativo per la gestione delle immagini usato dal sistema e dalla maggior parte delle applicazioni. Le vulnerabilità in questo ambiente possono potenzialmente colpire numerose applicazioni diverse. I file grafici sono generalmente considerati "sicuri" dai vari programmi e vengono aperti per default senza un avviso preventivo.
- *Unix* – Mac OS X è basato sui primi sistemi operativi Unix e ne incorpora grandi fette di codice. Molte applicazioni scritte per i diversi Unix e per sistemi simili a Unix possono essere eseguite su Mac OS X ed alcune di queste applicazioni sono utilizzate da Apple come parte del sistema operativo. Le vulnerabilità di queste applicazioni potrebbero essere corrette per Mac OS X con un ritardo considerevole rispetto a quanto avviene per il produttore originale.
- *Wireless* – Con una certa sorpresa di molti componenti della comunità che si occupa di sicurezza, sono state riportate vulnerabilità critiche che riguardano il sottosistema di rete wireless di Mac OS X. Queste vulnerabilità possono permettere attacchi da parte di prossimità che possono portare al controllo completo dei sistemi affetti. La natura del problema ha permesso agli aggressori di attaccare anche sistemi che non fanno parte della stessa rete logica da cui proviene l'attacco. Ulteriori problemi sono stati rilevati nel sottosistema di interfaccia wireless Bluetooth, con risultati simili a quelli precedentemente descritti.
- *Virus/Trojan* – Nell'anno appena trascorso sono stati scoperti i primi esempi di virus e trojan per piattaforme Mac OS X.
- *Altre* – Vi sono altre vulnerabilità che non rientrano in categorie ben definite.

Da notare che Apple di solito distribuisce gli aggiornamenti e le patch come aggiornamenti globali: un dato aggiornamento di sicurezza ingloberà quindi sia gli aggiornamenti critici, sia quelli di importanza minore.

M1.2 Riferimenti CVE

Vulnerabilità di Safari (incluse quelle zero-days)

Vulnerabilità del Rendering HTML -[CVE-2005-3705](#), [CVE-2006-1987](#), [CVE-2006-3505](#), [CVE-2006-3946](#)

Vulnerabilità di esclusione di sicurezza -[CVE-2005-2516](#), [CVE-2006-0399](#), [CVE-2006-0397](#), [CVE-2006-0398](#).

Vulnerabilità di ImageIO

SANS Top

La versione italiana è curata da Data Security - www.datasecurity.it

Vulnerabilità nel formato delle immagini -[CVE-2006-1469](#), [CVE-2006-1982](#), [CVE-2005-2747](#)

Vulnerabilità di prodotti di terze parti

Vulnerabilità ereditate -[CVE-2006-0384](#)

Vulnerabilità del driver Wireless

Vulnerabilità del driver WiFi -[CVE-2006-3509](#), [CVE-2006-3508](#), [CVE-2006-3507](#)

Virus e Trojan

Virus e Trojan –Trojan [OSX/Leap-A](#).

Altre vulnerabilità

[CVE-2006-3498](#), [CVE-2006-1450](#), [CVE-2006-1449](#), [CVE-2006-0848](#), [CVE-2005-2518](#), [CVE-2006-4394](#)

M 1.3 Come stabilire se si è a rischio

Qualsiasi installazione di default o non corretta di Mac OS X deve essere considerata vulnerabile. La seguente procedura serve a verificare se ci sono nuovi pacchetti disponibili.

1. Scegliete Preferenze di Sistema dal menu Apple.
2. Scegliete Aggiornamento Software dal menu Visualizza.
3. Cliccate Aggiorna Adesso.
4. Verificate le voci disponibili

Come aiuto nel processo di correzione delle vulnerabilità, potete contare su un qualsiasi vulnerability scanner.

M1.4 Come proteggersi da queste vulnerabilità

- Assicuratevi di essere al passo e di aver installato tutti gli aggiornamenti di sicurezza per i prodotti Apple attivando il sistema di Aggiornamento Software per controllare automaticamente gli aggiornamenti software rilasciati da Apple. Per quanto siano possibili differenti pianificazioni, vi raccomandiamo di configurare la verifica degli aggiornamenti almeno su base settimanale. Per maggiori informazioni su come attivare ed eseguire il sistema di Aggiornamento Software, consultate la pagina di Aggiornamenti Software di Apple all'indirizzo <http://www.apple.com/it/macosex/upgrade/softwareupdates.html>
- Per evitare accessi non autorizzati alla vostra macchina, attivate il personal firewall di sistema. Se sulla vostra macchina girano servizi autorizzati che hanno bisogno di un accesso esterno, assicuratevi di assegnare esplicitamente tali permessi.
- Vi sono molte guide eccellenti per l'hardening dei sistemi Mac OS X. Il [CIS Benchmark](#) per Mac OS X elenca le configurazioni di sicurezza utili a rendere sicuro il sistema operativo. Le azioni suggerite dai documenti benchmark CIS Level-1 difficilmente comportano interruzione di servizi o applicazioni, e quindi si raccomanda vivamente di applicarle. Anche il white paper [Securing Mac OS X 10.4 Tiger](#) prende in esame le funzionalità di sicurezza e i metodi per rendere sicuro Mac OS X.

U1. Configurazioni deboli di UNIX

U1.1 Descrizione

La maggior parte dei sistemi Unix/Linux include una serie di servizi standard nelle installazioni di default. Questi servizi, anche se completamente aggiornati, possono essere la causa di problemi non previsti. Gli amministratori più attenti alla sicurezza rafforzano i propri sistemi disabilitando i servizi non necessari e/o bloccando il loro accesso da Internet tramite sistemi firewall.

L'installazione di default di Red Hat Enterprise Linux, ad esempio, presenterà servizi come cups (Common Unix Printing System), portmap (supporto RPC), sendmail (Mail Transport Agent), e sshd (server OpenSSH) che, se non utilizzati, dovrebbero essere disabilitati.

Di particolare interesse sono gli **attacchi brute-force diretti verso servizi con accesso a linea di comando come SSH, FTP e telnet**. Questi servizi sono spesso obiettivo di attacco in quanto utilizzati prevalentemente per l'accesso da remoto. Nel corso degli ultimi due anni si è riscontrato un impegno comune da parte degli aggressori ad operare attacchi brute-force verso le password usate in queste applicazioni. Un numero sempre crescente di worm e bot contengono motori per attacchi brute force alle password. I sistemi con password deboli per gli account utente vengono messi in pericolo; spesso attraverso l'escalation di privilegi si riesce ad ottenere un accesso root e ad installare dei root-kit per nascondere le tracce. È importante ricordare che l'attacco brute force verso le password può essere una tecnica valida per compromettere anche quei sistemi che presentano tutti gli aggiornamenti di sicurezza necessari.

Gli amministratori più attenti alla sicurezza utilizzano SSH come sistema per interagire da remoto con i sistemi. Se la versione di SSH è quella più recente e con tutte le patch installate, si considera generalmente il servizio come sicuro. Ciononostante, per quanto sia recente o aggiornato, può essere ancora compromesso tramite attacchi brute-force che ne individuino le password. Per questo si consiglia di usare per SSH meccanismi di autenticazione a chiave pubblica, che sono in grado di evitare questo tipo di attacco. Per quanto riguarda i restanti servizi di interazione, verificate le password per accertarvi che presentino una complessità sufficiente a resistere ad attacchi brute-force.

U1.2 Versioni colpite

Tutte le versioni di UNIX/Linux sono potenzialmente a rischio a causa di configurazioni improprie o di default. Tutte le versioni di UNIX/Linux possono essere in pericolo se gli account di autenticazione usano password deboli o presenti in un dizionario.

U1.3 Come stabilire se si è vulnerabili

Le installazioni di default (sia che siano effettuate da un produttore o da un amministratore) di sistemi operativi o di applicazioni di rete possono introdurre una vasta gamma di servizi non necessari e non utilizzati. In molti casi l'indefinibilità a priori su cosa avrà davvero bisogno un sistema operativo o una applicazione porta molti produttori e amministratori a installare tutto il software a disposizione nel caso diventi utile in futuro. Questa pratica semplifica significativamente il processo di installazione ma introduce anche una vasta gamma di servizi non necessari e account con password di default, deboli o altrimenti conosciute.

L'uso di un vulnerability scanner aggiornato o di un port mapper può essere molto efficace per la scoperta di qualche vulnerabilità potenziale ereditata dalle installazioni di default o da servizi e applicazioni non necessarie e/o obsolete. Anche un password cracker può essere utile per evitare l'utilizzo di password deboli o di facile individuazione.

Attenzione: Non utilizzate mai un password cracker o un vulnerability scanner, neanche sui sistemi per i quali avete un accesso root, senza autorizzazione esplicita e preferibilmente scritta da parte del vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.

U1.4 Come proteggersi da queste vulnerabilità

Servizi non necessari

- Analizzate il server con un port scanner o uno strumento di vulnerability assessment per determinare quali servizi non necessari siano attivi sul sistema. Disabilitate i servizi che non sono richiesti da qualche applicazione necessaria.
- Installate regolarmente le più recenti patch rilasciate dal fornitore per attenuare le vulnerabilità nei servizi esposti. La gestione delle patch è una parte fondamentale del processo di gestione del rischio.
- Utilizzate i benchmark del Center for Internet Security (www.cisecurity.org) per i sistemi operativi e i servizio che utilizzate. Considerate anche l'utilizzo di Bastille per rafforzare gli host Linux e HP-UX (www.bastille-linux.org).
- Considerate la possibilità di trasferire i servizi dalle porte di default non appena possibile. Gli scanner automatici tendono ad analizzare solo le porte di default.
- Usate un firewall hardware o software per proteggere i servizi necessari.
- Assicuratevi che i servizi siano protetti da meccanismi di sicurezza forniti dal produttore (come ad esempio SELinux o address space randomization).

Attacchi Brute Force

- Non usate le password di default su alcun account.
- Attuate una politica di password robuste. Non permettete l'utilizzo di password deboli o che contengano parole presenti in un dizionario.
- Limitate gli account che possono accedere attraverso la rete; root non dovrebbe essere uno di questi.
- Implementate delle regole del firewall che limitino la fonte di tutti i login da remoto.
- Proibite l'utilizzo di account condivisi e non utilizzate nomi utente generici come tester, guest, sysadmin, admin, ecc.
- Conservate un registro dei tentativi di login falliti. Un numero alto di tentativi di login falliti a un sistema può richiedere un controllo ulteriore sul sistema vedere se è stato compromesso.
- Effettuate delle verifiche per accertarvi che la vostra politica di password sia rispettata.
- Limitate il numero di tentativi di login falliti possibile per i servizi più esposti.
- Prendete in considerazione un sistema di autenticazione basato su certificati.
- Se il vostro sistema UNIX permette l'uso di moduli di autenticazione PAM, implementate i moduli PAM per verificare la resistenza delle password.
- Bloccate tramite firewall i servizi che non richiedono accesso a Internet.

U1.5 Riferimenti

Attacchi Brute Force a SSH e relative contromisure

- <http://isc.sans.org/diary.php?storyid=1541>
- <http://isc.sans.org/diary.php?storyid=1491>
- <http://isc.sans.org/diary.php?date=2006-08-01>
- http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1094140,00.html

Risorse generali per la sicurezza di UNIX

- <http://www.cisecurity.org>
- <http://www.bastille-linux.org>
- <http://www.puschitz.com/SecuringLinux.shtml>

C1 Applicazioni Web

C1.1 Descrizione

Le applicazioni Web come i Content Management System (CMS), Wiky, Portali, Bulletin Board e forum di discussione sono utilizzate da organizzazioni grandi e piccole. Ogni settimana si riscontrano in queste applicazioni si scoprono **centinaia** di vulnerabilità, che vengono regolarmente sfruttate per attacchi. Il numero di tentativi giornalieri di attacco per alcuni dei maggiori fornitori di web hosting varia da **centinaia di migliaia fino a milioni**.

Tutti gli ambienti web f (PHP, .NET, J2EE, Ruby on Rails, ColdFusion, Perl, ecc) e qualsiasi tipologia di applicazione web è a rischio a causa di questi problemi di sicurezza che vanno da insufficienti mediti di validazione fino a errori nella logica dell'applicazione. Le vulnerabilità più sfruttate sono:

- **PHP Remote File Include:** PHP è il linguaggio e l'ambiente attualmente più utilizzato per applicazioni web. PHP permette per default l'accesso a risorse su Internet come se fossero file utilizzando una funzionalità chiamata "allow_url_fopen". Quando gli script PHP permettono all'utente inserimenti che interagiscano con i nomi dei file, è possibile che si verifichi l'inclusione di file remoti. Questo attacco permette (ma non solo):
 - L'esecuzione di codice da remoto

- L'installazione di root kit
- Su Windows, l'attacco al sistema attraverso l'uso dei file wrappers SMB di PHP
- **SQL Injection:** Le injection, in particolare le SQL injection, sono piuttosto comuni nelle applicazioni web. Le Injection sono rese possibili dalla mescolanza di dati forniti dall'utente con query dinamiche o all'interno di procedure mal costruite. Le SQL injection permettono ai malintenzionati di:
 - Creare, leggere, modificare o cancellare qualsiasi dato disponibile nell'ambito dell'applicazione
 - Nel peggiore dei casi, di compromettere completamente il sistema del database e i sistemi correlati
- **Cross-Site Scripting (XSS):** Il cross site scripting, meglio conosciuto come XSS, è il problema di sicurezza più pernicioso e maggiormente riscontrabile per le applicazioni web. XSS permette agli aggressori di deturpare i siti web, di inserire contenuti dannosi, di condurre attacchi di phishing, di prendere il controllo del browser degli utenti utilizzando codici JavaScript e posta gli utenti ad eseguire comandi non di loro scelta – un attacco conosciuto come *cross-site request forgery*, meglio noto come CSRF.
- **Cross-site request forgery (CSRF):** CSRF forza gli utenti legittimi ad eseguire comandi senza il loro consenso. Questo tipo di attacco è estremamente difficile da prevenire a meno che l'applicazione non sia esente da vettori cross-site scripting, comprese le DOM injection. Con la crescita della diffusione di tecniche Ajax e la conoscenza più approfondita su come sfruttare gli attacchi XSS, gli attacchi CSRF stanno diventando molto sofisticati, sia come attacco specifico attivo, sia come automatismo di web come il Samy MySpace Worm.
- **Directory Traversal:** Directory traversal (l'accesso ai file via ".." o tramite molte altre varianti) permette agli aggressori di accedere a risorse riservate, come ad esempio i file di password o di configurazione, credenziali di database o altri file scelti dall'aggressore.

C1.2 Come stabilire se si è a rischio

Gli strumenti di scansione Web possono aiutare a riscontrare queste vulnerabilità, specialmente se si tratta di bug conosciuti. Per trovare le vulnerabilità potenziali è però necessaria una revisione del codice sorgente. Questa operazione dovrebbe essere eseguita dallo sviluppatore prima del rilascio.

Controllare come è configurata la struttura della vostra applicazione web e operate le opportune sicurizzazioni.

Gli amministratori del sistema dovrebbero prevedere una scansione periodica dei web server tramite dei vulnerability scanner, in particolare quando questi ospitano una vasta gamma di script diversi forniti dagli utenti, come accade nelle hosting farm. Effettuare dei penetration test dettagliati diventa in questi casi un'opzione inapplicabile..

C1.3 Come proteggersi dalla vulnerabilità delle applicazioni web

Dal punto di vista dell'hosting e dell'amministratore del sistema PHP:

- Effettuate l'aggiornamento a PHP 5.2, in quanto questa versione elimina molti dei problemi di sicurezza di PHP e permette API più sicure come PDO.
- Provate e quindi installate le patch e le nuove versioni di PHP non appena vengono rilasciate
- Si raccomanda l'uso frequente di scansioni web in particolare per gli ambienti ove sono in uso una grande numero di applicazioni PHP.
- Verificate la possibilità di utilizzare le seguenti configurazioni di PHP:
 - register_globals dovrebbe essere off (interferirà con applicazioni insicure)
 - allow_url_fopen dovrebbe essere off (interferirà con applicazioni che utilizzano questa funzionalità, ma vi proteggerà da un vettore di attacchi molto dannoso)
 - magic_quotes_gpc dovrebbe essere off (interferirà con applicazioni insicure meno recenti)
 - open_basedir dovrebbe essere abilitato e correttamente configurato
- Verificate la possibilità di utilizzare funzionalità con privilegi di esecuzione molto bassi come PHPsuexec o suPHP

- Prendete in considerazione Suhosin per controllare l'ambiente di esecuzione degli script PHP
- Utilizzate sistemi di Intrusion Prevention/Detection per bloccare o segnalare richieste HTTP sospette. Prendete in considerazione mod_security di Apache per bloccare gli attacchi PHP noti
- Come ultima risorsa, prendere in considerazione il blocco delle applicazioni in cui sono state rilevate delle vulnerabilità sfruttate e rallentate i tempi di risposta per risolvere i problemi di sicurezza conosciuti.

Dal punto di vista dello sviluppatore:

- Se usate PHP, migrate rapidamente la vostra applicazione verso PHP 5.2.
- Per evitare i problemi di codifica illustrati:
 - o Sviluppate le applicazioni con la versione più recente di PHP e una configurazione sicura (vedi sopra)
 - o Validate in maniera appropriata tutti gli input
 - o Codificate tutti gli output usando htmlentities() o meccanismi simili per evitare gli attacchi XSS
 - o Migrate la parte dati verso PDO – non utilizzate le funzioni mysql_*() vecchio stile, notoriamente difettose
 - o Non usate funzioni in cui gli input dell'utente interagiscano con file, per evitare attacchi di remote file inclusion
- Associatevi alle organizzazioni per la codifica sicura come OWASP (vedi riferimenti) per sviluppare le vostre conoscenze e imparare a programmare in modo sicuro
- Provate le vostre applicazioni utilizzando la OWASP Testing Guide con strumenti quali WebScarab, la Web Developer Toolbar di Firefox, Greasemonkey e XSS Assistant

C1.4 Riferimenti

OWASP -Open Web Application Security Project

<http://www.owasp.org>

OWASP Testing Guide

http://www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents

OWASP Guide -a compendium of secure coding

http://www.owasp.org/index.php/Category:OWASP_Guide_Project

OWASP Top 10 -Top 10 web application security weaknesses

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Suhosin, a Hardened PHP project to control the execution environment of PHP applications

<http://www.hardened-php.net/suhosin/>

PHP Security Features

<http://php.net/features.safe-mode>

C2. Database Software

C2.1 Descrizione

I database sono un elemento chiave di molti sistemi in quanto immagazzinano, cercano o comunque manipolano una grande quantità di dati. Si trovano praticamente in qualsiasi tipo di business, in applicazioni finanziarie, bancarie, di relazione con il cliente e nei sistemi di monitoraggio.

Siccome nei database sono spesso conservate informazioni molto importanti come dati personali o finanziari, questi sono spesso obiettivo di attacchi e sono particolarmente ambiti dai ladri di identità. I sistemi

database sono spesso molto complessi e combinano l'applicazione principale con una serie di altre applicazioni, alcune fornite dagli stessi produttori del database, altre spesso scritte in casa (come le applicazioni web). Un difetto in uno di questi componenti può mettere in pericolo i dati contenuti. Le vulnerabilità più comuni nei sistemi database possono essere classificate come:

- Uso delle configurazioni di default con nomi utente e password di default.
- Buffer overflow in processi in ascolto su porte TCP/UDP ben conosciute.
- SQL Injection attraverso gli strumenti specifici del database o applicazioni web di front-end aggiunte dagli utenti.
- Uso di password poco sicure per account con privilegi alti

Esistono molti sistemi database diversi. Tra i più diffusi vi sono Microsoft SQL Server (proprietario, gira su Windows), Oracle (proprietario, gira su diverse piattaforme), IBM DB2 e IBM Informix (entrambi sistemi proprietari che possono girare su diverse piattaforme), Sybase (proprietario, gira su diverse piattaforme), MySQL e PostgreSQL (entrambi open source e utilizzabili su molte piattaforme).

Tutti i moderni sistemi database relazionali sono port addressable, il che significa che chiunque, con strumenti per la generazione di query di semplice reperimento può provare a connettersi direttamente al database, eludendo i sistemi di sicurezza utilizzati dai sistemi operativi. Le connessioni di default più comunemente utilizzate sono: Microsoft SQL attraverso la porta TCP 1433 e la porta UDP 1434, Oracle attraverso la porta TCP 1521, IBM DB2 attraverso la porta 523 e quelle dalla 50000 in su, IBM Informix attraverso le porte 9088 e 9099, MySQL attraverso la porta TCP 3306 e PostgreSQL attraverso la porta TCP 5432.

A riprova di ciò, su Internet si possono facilmente reperire exploit per molti banchi di database. A causa delle connessioni di rete che forniscono, i database possono inoltre essere colpiti da worm. Il più famigerato tra questi è il celebre [SQL Slammer worm](#) del 2003. Il 2005 vide poi l'affacciarsi del primo worm per Oracle: "[Voyager](#)". Anche se questo worm non trasportava codice dannoso, ha dimostrato ampiamente cosa può succedere a un database Oracle se questo non viene adeguatamente protetto.

Oltre a correggere le specifiche vulnerabilità menzionate in questo capitolo, I tecnici che hanno a che fare con la sicurezza dei database devono esaminare:

- Le implicazioni di standard quali il [Payment Card Industry Data Security Standard](#) che richiedono la crittografia per alcune informazioni quali i numeri delle carte di credito.
- I rischi derivanti dal trasferimento di grandi quantità di dati verso dispositivi mobili: nell'ultimo anno vi sono state numerose notizie di dati personali smarriti a causa del furto dei laptop in cui erano contenuti.

C2.2 Sistemi operativi colpiti

La maggior parte dei sistemi database, sia commerciali che open source, operano su diverse piattaforme. I problemi riguardano indistintamente tutte le piattaforme supportate.

C2.3 Riferimenti CVE

Quelle che seguono sono i riferimenti dall'ottobre 2005 in poi. Le vulnerabilità inserite precedentemente possono essere rilevate consultando le edizioni precedenti delle TOP20 SANS. Spesso i problemi non riguardano banchi specifici dei database, ma vulnerabilità nelle applicazioni accessorie, come, ad esempio, le SQL injection nelle interfacce web; questi casi non sono inseriti nel seguente elenco.

Oracle

[CVE-2005-3641](#), [CVE-2006-0256](#), [CVE-2006-0257](#), [CVE-2006-0258](#), [CVE-2006-0259](#), [CVE-2006-0260](#), [CVE-2006-0261](#), [CVE-2006-0262](#), [CVE-2006-0263](#), [CVE-2006-0265](#), [CVE-2006-0266](#), [CVE-2006-0267](#), [CVE-2006-0268](#), [CVE-2006-0269](#), [CVE-2006-0270](#), [CVE-2006-0271](#), [CVE-2006-0272](#), [CVE-2006-0282](#), [CVE-2006-0283](#), [CVE-2006-0285](#), [CVE-2006-0286](#), [CVE-2006-0287](#), [CVE-2006-0290](#), [CVE-2006-0291](#), [CVE-2006-0435](#), [CVE-2006-0547](#), [CVE-2006-0548](#), [CVE-2006-0549](#), [CVE-2006-0551](#), [CVE-2006-0552](#), [CVE-2006-0586](#), [CVE-2006-1868](#), [CVE-2006-1871](#), [CVE-2006-1872](#), [CVE-2006-1873](#), [CVE-2006-1874](#), [CVE-2006-3698](#).

Nota: Questa lista si limita ai programmi fondamentali del database Oracle. Sono presenti però altre vulnerabilità in altre applicazioni che compongono la suite Oracle. Oracle pubblica trimestralmente una Critical Patch Update (CPU) che corregge i problemi riscontrati nelle applicazioni database e in quelle

correlate. Il consiglio è di operare utilizzando queste CPU. Siccome Oracle ha pubblicato diverse informazioni durante il periodo preso in considerazione, molte voci CVE possono riguardare un singolo problema.

MySQL

[CVE-2006-2753](#).

PostgreSQL

[CVE-2006-2313](#), [CVE-2006-2314](#).

IBM DB2

[CVE-2005-3643](#), [CVE-2005-4737](#).

IBM Informix

[CVE-2005-3642](#), [CVE-2006-3854](#), [CVE-2006-3860](#), [CVE-2006-3862](#).

Microsoft SQL Server

Nessuna nel periodo esaminato.

Sybase

Nessuna nel periodo esaminato.

C2.4 Come stabilire se si è vulnerabili

Non basta controllare una semplice lista manuale delle applicazioni installate! Siccome i database sono spesso distribuiti quali componenti di altre applicazioni, capita spesso di installare un database senza rendersene conto. I database possono di conseguenza rimanere privi di patch e aggiornamenti o con le vulnerabilissime configurazioni di default. Questo fatto è stato efficacemente dimostrato quando il worm SQL Slammer ha attaccato il Microsoft Data Access Component (MDAC), che è contenuto in diversi programmi.

Eseguite una scansione delle vulnerabilità sui sistemi per stabilire quali software DBMS software sono attivi, accessibili e vulnerabili. Potete utilizzare vulnerability scanner generali o strumenti forniti dai produttori di database come [MySQL Network Scanner](#) o [Microsoft SQL server tool](#). Per Microsoft SQL Server si può usare anche il [Microsoft Baseline Security Analyzer](#).

C2.5 Come proteggersi dalla vulnerabilità dei database

- Controllate che tutti i DBMS siano aggiornati con le patch più recenti. Le versioni obsolete o non corrette molto probabilmente presentano delle vulnerabilità. Controllate spesso il sito del produttore per le informazioni sulle patch. Tenetevi aggiornati riguardo le vulnerabilità e gli avvisi pubblicati dai produttori:
 - Avvisi di sicurezza Oracle (<http://www.oracle.com/technology/deploy/security/alerts.htm>)
 - MySQL (<http://lists.mysql.com/>)
 - PostgreSQL (<http://www.postgresql.org/support/security>)
 - Microsoft SQL (<http://www.microsoft.com/technet/security/bulletin/notify.mspx>)
 - IBM DB2 (<http://www-306.ibm.com/software/data/db2/udb/support/>)
 - IBM Informix (<http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg24009130>)
- Assicuratevi che i DBMS e le applicazioni siano stati messi al sicuro:
 - Eliminate/cambiate le password di default per gli account di sistema e del database con privilegi alti prima di mettere il sistema in rete. Le liste degli account di default sono facilmente reperibili su Internet.
 - Assegnate i privilegi strettamente indispensabili
 - Quando possibile, usate le stored procedure.

- Eliminate/disabilitate le stored procedure non necessarie.
- Impostate dei limiti alla lunghezza di tutti i campi dei form.
- Consultate la sezione Riferimenti seguente, che indica molte risorse utili per rendere sicuri i DBMS.
- Usate dei firewall o altri dispositivi per la sicurezza delle reti per limitare gli accessi alla porte associate ai servizi database.
- Non fidatevi degli inserimenti degli utenti! Assicuratevi che le applicazioni collegate al database effettuino una pulizia sul lato server di tutti gli input per evitare attacchi come le SQL injection (vedi <http://www.sans.org/rr/whitepapers/securecode/23.php>)

C2.6 Riferimenti

Risorse generali e per vari database

- La sezione SANS sulla sicurezza dei database: http://www.sans.org/rr/catindex.php?cat_id=3
- La guida DoD sulle tecniche per rendere sicuri i database security: <http://iase.disa.mil/stigs/stig/databasestig-v7r2.pdf>
- <http://www.databassecurity.com/>

Oracle

- L'esauriente Checklist SANS per la sicurezza di Oracle: <http://www.sans.org/score/oraclechecklist.php?portal=380f9e4dc7f96d133a6282b28252a0f0>
- https://store.sans.org/store_item.php?item=80
- http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
- CIS benchmark tool: http://www.cisecurity.org/bench_oracle.html
- <http://www.petefinnigan.com/orasec.htm>
- <http://otn.oracle.com/deploy/security/index.html>
- <http://www.red-database-security.com/>

MySQL

- La guida passo-passo di SecurityFocus per la sicurezza di MySQL: <http://www.securityfocus.com/infocus/1726>
- <http://dev.mysql.com/doc/mysql/en/Security.html>

Guida per rendere sicuro PostgreSQL

- <http://www.postgresql.org/support/security>
- <http://www.postgresql.org/docs/techdocs.53>

Sicurezza di Microsoft SQL

- <http://www.microsoft.com/sql/techinfo/administration/2000/security/default.msp>
- <http://www.sqlsecurity.com/>
- CIS SQL Server Benchmark Tool: http://www.cisecurity.org/bench_sqlserver.html

IBM DB2

- http://www.net-security.org/dl/articles/Securing_IBM_DB2.pdf

IBM Informix

- <http://www.databassecurity.com/informix.htm>

- <http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.admin.doc/admin197.htm>

Sybase

- Guida alla sicurezza di Sybase: <http://www.niiconsulting.com/innovation/Sybase.pdf>

C3. Applicazioni per la condivisione P2P

C3.1 Descrizione

Le reti Peer to Peer sono costituite da una serie di computer o “nodi” che funzionano simultaneamente da “client” e da “server” per raggiungere un intento comune. I nodi possono scambiarsi dati, condividere risorse, fornire servizi di directory, sostenere comunicazioni e fornire strumenti per la collaborazione in tempo reale.

Possono essere utilizzate molte architetture di controllo e comunicazione. Talvolta vengono utilizzati dei server di indicizzazione centralizzati che forniscono i servizi di ricerca dei dati e dei servizi disponibili. Nelle reti completamente distribuite ciascun nodo collabora a servizi di indicizzazione e di ricerca ed è del tutto equivalente ad un altro nodo. Le architetture ibride, invece, combinano le caratteristiche dei due modelli in differenti gradazioni: gruppi di nodi possono “scegliere/promuovere” determinati nodi per fungere da server di indicizzazione e di ricerca in una determinata zona.

Molte applicazioni legali usano il P2P. Alcuni produttori di software, tra i quali Microsoft e Sun, propongono diversi strumenti per utilizzarle e incoraggiano lo sviluppo di applicazioni P2P. Tuttavia le applicazioni P2P, come qualsiasi altro strumento per il trasferimento di informazioni, possono portare a usi non corretti o sfruttate per condividere illegalmente materiale soggetto a diritto d'autore, per ottenere dati riservati, per inviare agli utenti materiale pornografico, violento o propagandistico, per distribuire ed eseguire codice dannoso (virus, spyware, bot, ecc.), per sovraccaricare la rete, per tracciare usi e modelli di comportamento degli utenti: tutte azioni che possono comportare una responsabilità nei confronti delle leggi. La responsabilità legale e la conseguente perseguibilità possono in certi casi non essere limitate al singolo esecutore, ma essere estese al promotore, ai sostenitori e ai membri della rete.

Le stesse reti P2P possono essere vittima di attacchi che possono sostituire file legittimi tramite con codici dannosi, seminando questi malware nelle directory condivise, che sfruttano errori di codice o le vulnerabilità insite nel protocollo che portano a bloccare (filtering) il protocollo, che raggiungono effetti di denial of service portando la rete a funzionare molto lentamente, che producono spamming e attacchi d'identità che portano ad identificare gli utenti della rete per poi perseguirli. Alcune azioni legali hanno portato alla chiusura di alcune reti molto popolari, colpevoli di aver infranto le normative che regolano i diritti d'autore..

I concetti e le tecniche P2P sono in contesa evoluzione e si possono trovare in:

- Reti per la condivisione di file (*file sharing*) — il cui obiettivo primario è quello di condividere risorse quali la memoria e la banda. Queste operano attraverso una rete distribuita di client, condividendo cartelle di file o interi dischi di dati. I client partecipano scaricando i file dagli altri utenti, rendendo disponibili agli altri i propri dati e coordinando per gli altri utenti le ricerche di file
- Cloud Computing — (conosciuto anche come elaborazione distribuita, Grid Computing, o reti mesh) dove “nuvole” di computer sono dedicate a fornire un ambiente virtuale di calcolo per compiere determinate operazioni distribuendo i dati e il carico di elaborazione. Il Cloud Computing inserisce i server in linea a seconda delle esigenze e l'utente finale non sa dove i dati risiedono o vengano elaborati in quel momento. In alcuni casi l'applicazione viene eseguita in parte sui server e in parte sui PC degli utenti. I server cloud possono risiedere fisicamente presso grandi strutture controllate da una organizzazione o in qualunque luogo in Internet. Poiché la potenza di calcolo modulabile si basa sui server virtuali, il proprietario dei dati non sa mai dove questi dati o i suoi programmi risiedono fisicamente davvero.

La maggior parte dei programmi P2P usano una serie di porte di default, ma possono essere automaticamente o manualmente configurati per usare porte diverse quando è necessario aggirare sistemi di rilevamento, firewall o filtri in uscita. La tendenza sembra essere quella di andare verso l'uso dei wrapper http e della crittografia per aggirare le restrizioni aziendali.

C3.2 Sistemi operativi interessati

Sono presenti versioni dei software P2P per tutti i sistemi operativi Microsoft Windows attualmente in uso, lo stesso vale per Linux, MacOS e la maggior parte dei sistemi operativi Unix.

C3.3 Rilevare l'attività P2P

Rilevare l'attività P2P sulla rete può risultare impegnativo. È possibile individuare software P2P che girano sulla vostra rete nei seguenti modi:

- Monitorando il traffico sulle porte comunemente utilizzate dai software P2P. Alcuni programmi, però, hanno iniziato ad usare http, https e altre porte che di solito hanno bisogno di essere aperte nei firewall e nei proxy.
- Usando un application layer per protocolli P2P, che può identificare i programmi che usano le porte di solito permesse (come la porta 53 o la porta 80). Anche questo, però, fallisce quando programmi più scaltri usano la crittografia per il traffico che veicolano.
- Usando alcuni intrusion prevention software host based e strumenti di system change auditing, che possono prevenire l'installazione o l'esecuzione di applicazioni P2P assieme ad altro codice indesiderato.
- Tramite alcuni sistemi di Intrusion Detection con funzioni di pattern matching / behavioral, che possono identificare potenziali membri P2P. I pattern osservati includono la frequenza, il timing e la dimensione dei flussi di comunicazione.
- Effettuando delle scansioni della rete e della memoria dei PC alla ricerca dei contenuti normalmente scaricati dagli utenti P2P, ovvero *.mp3, *.wma, *.avi, *.mpg, *.mpeg, *.jpg, *.gif, *.zip, *.torrent, and *.exe.
- Quando intervengono dei cambiamenti nelle performance della rete possono indicare picchi dovuti all'uso di P2P o a infezioni causate da malware.
- Alcuni Firewall e prodotti di Intrusion Detection/Prevention combinano diverse tecniche di detection per rilevare o prevenire il traffico P2P in ingresso o in uscita dalla rete.
- Nelle macchine Microsoft Windows è possibile utilizzare SMS per analizzare gli eseguibili installati nelle workstation. Oltre a ciò, gli amministratori dovrebbero limitare i permessi in modo da impedire agli utenti di installare i software P2P sulle loro workstation.
- I sistemi compromessi che hanno dei malware installato via file sharing P2P mostreranno gli stessi sintomi rilevati quando sono vittime di malware diffuso con altri metodi.

C3.4 Come proteggersi dalle vulnerabilità che derivano dai software P2P

- Agli utenti standard non dovrebbe essere consentita l'installazione di software. Limitate i privilegi di Amministratore e Power User al personale di supporto per le loro funzioni tecniche. Se un utente ha bisogno di privilegi di Amministratore o Power User, creategli anche un diverso account da utilizzarsi per il normale lavoro di ufficio, per la navigazione web e la comunicazione on-line.
- Usate strumenti come [DropMyRights](#) di Microsoft o rendere sicuri i browser web e i client mail.
- In ambienti Active Directory è possibile usare le Software Restriction Policy per bloccare l'esecuzione di tipi noti di file binari.
- Sensibilizzate gli utenti riguardo le reti P2P, sottolineando i pericoli del file sharing e illustrando le politiche aziendali in proposito.
- Abilitate i filtri in uscita per limitare tutte le porte non necessarie alle attività aziendali, ma considerate il fatto che molte applicazioni P2P si stanno spostando verso l'http e la crittografia, rendendo meno efficace questa misura.
- Monitorate i log del firewall e dell'IDS.
- Per ridurre le infezioni da malware che possono essere diffuse da numerose applicazioni P2P, usate prodotti antispyware e antivirus in tutta l'azienda e assicuratevi che siano aggiornati quotidianamente.

- Usate firewall host-based oltre ai firewall perimetrali. Windows XP e Windows 2003 comprendono un firewall Windows che fornisce, se adeguatamente configurato, una buona protezione. Molti firewall host based di terze parti (ZoneAlarm, Sygate, Outpost) offrono ulteriori funzionalità e flessibilità. I sistemi Windows 2000, XP e 2003 possono utilizzare anche le policy IPSec, che forniscono una funzione di filtro delle porte rispetto al traffico non necessario sulle VPN. In ambienti Active Directory, le policy IPSec e la configurazione di Windows Firewall (per Windows XP SP2 e Windows 2003 SP1) possono essere gestite in maniera centralizzata tramite le Group Policy.
- Disabilitate la funzione *Condivisione file semplice* (Simple File Sharing) in Windows XP se non assolutamente necessaria [Start -Impostazioni –Pannello di controllo –Opzioni Cartella - Visualizzazione –Deselezionate l'impostazione *Condivisione file semplice* – Applica - OK.]
- Monitorate i sistemi alla ricerca di eseguibili non conosciuti e modifiche non autorizzate dei file di sistema. Si può utilizzare prodotti software come Tripwire o AIDE (c'è una versione commerciale e una open source) per verificare i cambiamenti nei file.
- Le condivisioni basate su Samba possono essere configurate per eseguire dei filtri sull'apertura o sul salvataggio dei file. Un filetype detector e un sistema di avvisi possono essere utili per prevenire l'abuso delle condivisioni.

C3.5 Riferimenti

Voce Peer-to-peer Wikipedia

<http://it.wikipedia.org/wiki/Peer-to-peer>

Sito sul Cybercrime del Dipartimento di Giustizia USA:

<http://www.usdoj.gov/criminal/cybercrime>

Altri fornitori di software che possono essere coinvolti in problemi legali legati al diritto d'autore.

[http://www.usdoj.gov/criminal/cybercrime/2006IPTFProgressReport\(6-19-06\).pdf](http://www.usdoj.gov/criminal/cybercrime/2006IPTFProgressReport(6-19-06).pdf)

Una iniziativa didattica dell'FBI <http://www.fbi.gov/cyberinvest/cyberedletter.htm>

The Information Factories http://www.wired.com/wired/archive/14.10/cloudware_pr.html

Mobile Service Clouds: A Self-managing Infrastructure for Autonomic Mobile Computing Services

<http://www.cse.msu.edu/~farshad/publications/conferences/samimi06msc.pdf>

Cyber Security Tip ST05-007 –Rischi della tecnologia per il File-Sharing

<http://www.us-cert.gov/cas/tips/ST05-007.html>

Rischi del File Sharing P2P (Presentazione)

<http://www.ftc.gov/bcp/workshops/filesharing/presentations/hale.pdf>

Protezione di Windows XP Professional in un ambiente di rete peer-to-peer

http://www.microsoft.com/italy/technet/security/smallbusiness/prodtech/windowsxp/sec_winxp_pro_p2p.mspx

Identificare gli utenti P2P con l'analisi del traffico -Yiming Gong -2005-07-21

<http://www.securityfocus.com/infocus/1843>

Bot software looks to improve peerage

<http://www.securityfocus.com/news/11390>

Fermare i bot

<http://www.securityfocus.com/columnists/398/1>

Blocco di specifici protocolli di rete e porte utilizzando IPSec

<http://support.microsoft.com/kb/813878>

Utilizzo delle Software Restriction Policy per proteggersi dal software non autorizzato

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx>

Disponibilità e la descrizione dello strumento Reporter Porta

<http://support.microsoft.com/kb/837243>

Nuove funzionalità e funzionalità in PortQry versione 2.0

<http://support.microsoft.com/default.aspx?kbid=832919>

Log Parser 2.2

<http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.msp>

Browsing the Web and Reading E-mail Safely as an Administrator (DropMyRights)

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp>

Amazon Cloud Computing goes beta

<http://www.amazon.com/gp/browse.html?node=201590011>

Checkpoint Application Intelligence

http://www.checkpoint.com/products/downloads/applicationintelligence_whitepaper.pdf

Ricerca sul sito Microsoft riguardo il peer-to-peer

<http://search.msdn.microsoft.com/search/default.aspx?siteId=0&tab=0&query=peer-to-peer>

Vulnerabilità dei sistemi di Instant-Messaging e P2P-per il settore sanitario

<http://ezinearticles.com/?Instant-Messaging-and-P2P-Vulnerabilities-for-Health-Organizations&id=232800>

Scovare e capire i Rootkit

<http://www.buanzo.com.ar/sec/Rootkits.html>

Application Layer Packet Classifier per Linux

<http://l7-filter.sourceforge.net/>

C4. Instant Messaging

C4.1 Descrizione

L'uso diffuso dell'instant messaging (IM) contribuisce ad aumentare i rischi di sicurezza sia per le aziende, sia per gli utenti individuali. Per quanto i sistemi di instant messaging possano rappresentare uno strumento di comunicazione estremamente utile, sono anche soggetti a molti problemi di sicurezza. Gli attacchi più recenti presentano nuove varianti nella costituzione e nella diffusione dei botnet e l'utilizzo degli account di instant messaging colpiti porta gli utenti a rivelare informazioni critiche. Attraverso gli instant message si diffondono anche alcune varianti di worm per e-mail (come quelli della famiglia di Mytob). Le aree di rischio legate agli instant message sono:

- Malware --Worm, virus e Trojan veicolati tramite l'uso degli instant message. Molti bot sono controllati attraverso canali IRC.
- Confidenzialità delle informazioni –Le informazioni trasmesse via instant messaging possono essere soggette a divulgazione in qualsiasi parte del processo di messaging.
- Rete – Attacchi di denial of service; eccessivo uso delle capacità della rete, anche quando l'utilizzo è legittimo.
- Vulnerabilità applicative – Le applicazioni di instant messaging presentano spesso vulnerabilità che possono essere sfruttate per attaccare i sistemi che le ospitano.

Le applicazioni più diffuse di instant message comprendono: AOL Instant Messenger (AIM), Gaim, ICQ, Jabber Messenger, Lotus Sametime, Skype, QQ, Windows Live Messenger (WLM), Google Talk, Trillian e Yahoo! Messenger. I protocolli di instant messaging sono IRC, MSNP, OSCAR, SIMPLE, XMPP e YMSG.

C4.2 Sistemi operativi interessati

Le applicazioni di instant messaging sono disponibili per tutti i sistemi operativi più diffusi.

C4.3 Voci CVE

[CVE-2006-0992](#), [CVE-2006-4662](#), [CVE-2006-5084](#)

C4.4 Come proteggersi dalle vulnerabilità e dall'uso non autorizzato dell'Istant Messaging

- Stabilite delle politiche sull'uso accettabile dell'istant messaging ed assicuratevi che tutti gli utenti siano informati riguardo a tali politiche, che le abbiano comprese chiaramente e siano consci dei potenziali rischi legati a queste applicazioni
- Agli utenti standard non dovrebbe essere permessa l'installazione di software. Limitate i livelli di privilegi di Amministratore e Power User al personale tecnico e solo per le loro incombenze di supporto e manutenzione dei sistemi. Se un utente ha bisogno di privilegi da Amministratore o Power User, create anche un account separato che venga utilizzato per il quotidiano lavoro di ufficio, la navigazione in Internet e le comunicazioni on-line.
- Controllate le patch fornite dai produttori siano prontamente applicate, sia per i software di instant messaging, sia per le applicazioni ad essi correlate, sia per i sistemi operativi che le ospitano.
- Adoperate prodotti antivirus e antispyware.
- Non affidatevi a server IM esterni per l'uso interno di instant messaging; installate un IM proxy o un IM server interno.
- Create canali di comunicazione sicura per utilizzare l'istant messaging con business partner riconosciuti.
- Configurate in modo appropriato i sistemi di intrusion detection/prevention. Ricordate che molte applicazioni di instant messaging sono in grado di abilitare comunicazioni associate per simulare una comunicazione consentita (es. http).
- Prendete in considerazione l'uso di prodotti specificamente progettati per la sicurezza dell'istant messaging.
- Filtrate tutto il traffico http attraverso un proxy server autenticato per avere la possibilità di usare risorse aggiuntive per il filtro o il monitoraggio del traffico generato dall'istant messaging.
- Bloccate l'accesso ai noti server pubblici di instant messaging che non siano esplicitamente autorizzati. (Nota: questa contromisura offre una protezione relativa, dato l'alto numero di potenziali server esterni)
- Bloccate le porte più comunemente utilizzate dall'istant messaging. (Nota: questa contromisura offre solo una protezione parziale, in quanto sono molti i protocolli possibili e le porte ad essi correlate, tenendo conto anche della capacità di alcune applicazioni di eludere alcune restrizioni relative alle porte.)
- Monitorate tramite un sistema di Intrusion Detection/Prevention l'attività di utenti che creano tunnel o eludono i proxy per l'Istant Messaging.

C4.5 Riferimenti

Phishers hijack IM accounts

http://news.com.com/Phishers+hijack+IM+accounts/2100-7349_3-6126367.html

Rich presence: a new user communications experience

http://www.alcatel.com/doctypes/articlepaperlibrary/html/ATR2005Q1/ATR2005Q1A17_EN.jhtml

Instant messaging: a new target for hackers

http://www.leavcom.com/ieee_july05.htm

AIM bot creates "fight combos" to spread

<http://www.securityfocus.com/brief/305>

Secure Instant Messaging in the Enterprise

http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1199405,00.html

C5. Lettori multimediali

C5.1 Descrizione

I lettori multimediali sono usati comunemente ed sono installati su milioni di sistemi. I contenuti vengono scaricati in forma di file multimediali quali film, video o musica. Questi contenuti sono anche inclusi in pagine Web e presentazioni o integrati in applicazioni multimediali.

I lettori multimediali possono essere presenti sui sistemi attraverso le installazioni di default o inclusi in altri software. Normalmente i browser sono impostati per scaricare ed aprire in modo "confortevole" i file multimediali senza richiedere una interazione da parte dell'utente. Spesso lettori e contenuti multimediali vengono scaricati dagli utenti sulle reti aziendali, per facilitare il trasferimento di contenuti sui propri dispositivi portatili.

Nell'anno appena trascorso sono state scoperte una serie di vulnerabilità in diversi lettori multimediali. Molte di queste vulnerabilità permettono a pagine web create ad arte o a file multimediali di pregiudicare completamente la sicurezza dei sistemi senza richiedere molti interventi da parte dell'utente. I sistemi possono essere colpiti semplicemente visitando alcune pagine web. Queste vulnerabilità, inoltre, possono essere sfruttate per installare software dannosi quali spyware, Trojan, adware o keylogger. In molti casi il codice che sfrutta tali vulnerabilità è disponibile pubblicamente.

Tra i più diffusi lettori multimediali troviamo:

- Windows: Windows Media Player, RealPlayer, Apple Quicktime, Winamp, iTunes
- Mac OS: RealPlayer, Quicktime, iTunes
- Linux/Unix: RealPlayer, Helix Player

C5.2 Sistemi operativi coinvolti

- Microsoft Windows
- Linux/UNIX
- Mac OS X

C5.3 Voci CVE

RealPlayer e Helix Player

[CVE-2006-1370](#), [CVE-2006-0323](#), [CVE-2005-2922](#), [CVE-2005-4130](#), [CVE-2005-4126](#), [CVE-2005-3677](#), [CVE-2005-2936](#)

iTunes

[CVE-2006-1249](#), [CVE-2005-4092](#), [CVE-2005-2938](#)

Winamp

[CVE-2006-0708](#), [CVE-2005-3188](#), [CVE-2005-2310](#)

Quicktime

[CVE-2006-2238](#), [CVE-2006-1456](#), [CVE-2006-1249](#), [CVE-2005-3713](#), [CVE-2005-3711](#), [CVE-2005-3710](#), [CVE-2005-3709](#), [CVE-2005-3708](#), [CVE-2005-3707](#), [CVE-2005-2340](#), [CVE-2005-4092](#), [CVE-2005-2743](#)

Windows Media Player

[CVE-2006-0025](#), [CVE-2006-0006](#), [CVE-2005-3591](#)

Macromedia Flash Player

[CVE-2005-3591](#), [CVE-2005-2628](#)

C5.4 Come stabilire se si è vulnerabili

Se si utilizza uno qualsiasi dei lettori elencati e non si dispone della versione più recente aggiornata con tutte le patch a disposizione si è vulnerabili ai relativi attacchi. Una revisione periodica del software installato può essere utile per scoprire installazioni non desiderate di lettori multimediali come di installazioni abusive da parte degli utenti.

C5.5 Come proteggersi dalle vulnerabilità dei lettori multimediali

Quelli che seguono sono alcuni dei metodi più comuni per difendersi da queste vulnerabilità:

- Aggiornate i lettori multimediali con tutte le patch più recenti. La maggior parte dei player fornisce un servizio di aggiornamento raggiungibile dai menu di aiuto o degli strumenti.
- Controllate con cura le installazioni standard di sistemi operativi e di altri prodotti software e verificate che non includano lettori multimediali che non desiderate installare. Configurate i sistemi operativi e i browser in modo da vietare installazioni non intenzionali.
- Usate sistemi di Prevention/Detection e software Anti-virus e di rilevamento Malware per bloccare i file multimediali pericolosi.
- Quando possibile, impedite l'installazione da parte degli utenti di software scaricato dalla rete sui client aziendali. Questa pratica vi faciliterà la gestione delle patch e la prevenzione delle vulnerabilità
- Non installate lettori multimediali sui sistemi sui quali non devono essere eseguiti file multimediali (ad esempio sui server)

C5.6 Riferimenti

La sezione sui lettori multimediali del sito RealNetworks

http://www.realnetworks.com/products/media_players.html

Security Report

<http://service.real.com/help/faq/security/>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=40#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=39#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely2>

Home Page di Helix Player

<https://player.helixcommunity.org/>

Notizie e annunci relativi alla sicurezza

<https://helixcommunity.org/news/>

Security Report

<http://www.sans.org/newsletters/risk/display.php?v=4&i=40#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=39#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely2>

Home Page di Apple QuickTime

<http://www.apple.com/quicktime/>

Home page di Apple iTunes

<http://www.apple.com/itunes/>

Aggiornamenti di sicurezza di Apple

<http://docs.info.apple.com/article.html?artnum=61798>

Supporto QuickTime

<http://www.apple.com/support/quicktime/>

Security Report

<http://www.sans.org/newsletters/risk/display.php?v=5&i=39#06.39.25>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=37#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=27#06.27.34>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=26#widely4>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=19#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=11#06.11.28>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=2#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=49#05.49.24>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely2>

Nullsoft Winamp

<http://www.winamp.com/>

Notizie e annunci relativi alla sicurezza

<http://www.winamp.com/about/news.php>

Security Report

<http://www.sans.org/newsletters/risk/display.php?v=5&i=25#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=8#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely4>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=5#widely1>

Home page di Microsoft Windows Media Player

<http://www.microsoft.com/windows/windowsmedia/default.aspx>

Sicurezza di Windows Media Player 10

<http://www.microsoft.com/windows/windowsmedia/mp10/security.aspx>

Microsoft Security Bulletin Search

<http://www.microsoft.com/technet/security/current.aspx>

Security Report

<http://www.sans.org/newsletters/risk/display.php?v=5&i=24#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=7#widely3>

Homepage di Macromedia Flash Player

<http://www.macromedia.com/software/flashplayer>

Security Report

<http://www.sans.org/newsletters/risk/display.php?v=5&i=42&rss=Y#06.42.23>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=37#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=28#widely8>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=19#widely5>

<http://www.sans.org/newsletters/risk/display.php?v=5&i=11#06.11.27>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=46#05.46.29>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely3>

C6. Server DNS

C6.1 Descrizione

Il Domain Name System (DNS) è un meccanismo fondamentale di Internet che serve soprattutto ad agevolare la conversione tra nomi degli host univoci verso i corrispondenti indirizzi IP (Internet Protocol) univoci usando una formula di database distribuito. Il DNS si basa su un modello di riservatezza sviluppato in un'era di fiducia reciproca molto diversa da quella attuale, in cui Internet è spesso poco amichevole. Il cambiamento della natura di Internet ha portato il DNS ad essere perseguitato da molti tipi di attacchi che sono facilitati da quella fiducia e che comprendono il *cache poisoning*, il *domain hijacking* e il *man-in-the-middle redirection*.

Durante l'anno appena trascorso, i botnet (reti di computer collegati ad internet che, a causa di falle nella sicurezza, vengono infettati da codici i quali consentono ai loro creatori di controllare i sistemi da remoto) hanno portato verso i server DNS i seguenti tipi di attacco:

1. **Attacchi di Denial of Service ricorsivo:** Il Botmaster (ovvero colui che controlla la botnet) pubblica un grande record DNS su un server DNS compromesso o allestito a tale scopo. Il botmaster quindi organizza la botnet per trasmettere piccole richieste UDP/53 ai server DNS ricorsivi pubblici (ovvero quelli configurati per processare non solo le richieste di Domain Name che hanno nel proprio database o in cache, ma anche le altre, interrogando altri server DNS), con un indirizzo di ritorno che rimanda alla vittima designata. Il risultato è che sono i server DNS, più che i bot, ad attaccare la vittima. L'effetto può essere poi ulteriormente amplificato da record DNS più grandi di un tipico pacchetto di risposta UDP/53, il che porta a forzare una richiesta sulla porta TCP/53.
2. **Spoofing Authoritative zone Answers:** Il botmaster mette in rete un sito web contraffatto (sito di phishing) su un server web compromesso. Il botmaster quindi organizza la botnet in modo che invii delle richieste a server DNS di una particolare zona, falsificando le risposte e puntandole verso il web server compromesso. Una variante di questo attacco è quella di agire localmente sui computer infettati dai bot e modificare i file host locali inserendo record che puntano all'indirizzo del sito web contraffatto.

C6.2 Come stabilire se si è a rischio

Tutti gli utenti di Internet rischiano di ottenere dati non corretti come risposta a query DNS. Se analizzando i server di cui avete la responsabilità risulta che questi non hanno installate le versioni più recenti o le ultime patch rilasciate dal fornitore del relativo software DNS, i vostri DNS server sono a rischio.

Un approccio proattivo per gestire la sicurezza di qualsiasi DNS server consiste nell'isciversi a uno degli avvisi personalizzati o a report delle vulnerabilità come quelle forniti da SANS, Secunia e altri o, in alternativa, di guardare con attenzione ciascun avviso inserito nell'Open Source Vulnerability Database (<http://www.osvdb.org>). Oltre agli avvisi di sicurezza, anche un vulnerability scanner aggiornato può essere molto efficace nel diagnosticare qualsiasi vulnerabilità potenziale nei server DNS. Inoltre si dovrebbe rivedere e testare la configurazione dei DNS server per assicurarsi che non siano permessi recursion o aggiornamenti inappropriati.

C6.3 Come proteggersi dalle vulnerabilità DNS

Come per qualsiasi pacchetto software, anche per i software per DNS Server devono essere installati gli aggiornamenti e le patch non appena questi sono disponibili e subito dopo averli testati in modo da accertarsi che non abbiano conseguenze sulle operazioni compite nella rete locale..

Per proteggersi dalle vulnerabilità DNS:

- Applicate tutte le patch del fornitore e aggiornate i server DNS all'ultima versione disponibile. Per maggiori informazioni su come rafforzare una installazione DNS, consultate gli articoli che spiegano come rendere sicuri i name services riportati nei benchmark del [Center for Internet Security DNS BIND](#) e nei corrispondenti benchmark del CIS per la vostra piattaforma operativa.
- Applicate regole appropriate nei firewall per tutti i server DNS interni alla rete che non hanno bisogno di essere accessibili da Internet.
- In Unix, per evitare un servizio DNS compromesso metta in pericolo l'intero sistema, restringete il servizio in modo che operi come utente senza privilegi speciali in una directory chroot(jed (jail)).

- Non permettete che i vostri recursive DNS server siano utilizzati al di fuori della vostra rete, a meno che ciò non sia strettamente necessario. Tale possibilità può essere evitata nella maggior parte dei casi agendo sulle configurazioni dei DNS o utilizzando regole dei firewall. Disabilitare le *recursion* e il *glue fetching* aiuta a difendersi dai DNS cache poisoning.
- Per rendere sicuri i *zone transfer* tra un DNS primario e uno secondario con un sistema crittografico, configurate i server in modo che utilizzino le DNS Transaction Signatures (TSIG). Prendete in considerazione la possibilità di firmare la vostra intera zona usando le DNS Security Extensions (DNSSEC).
- Su molti sistemi che usano BIND, il comando "named -v" mostrerà la versione installata numerata come X.Y.Z dove X è la versione principale, Y la versione secondaria e Z il livello di patch. Attualmente le due versioni principali di BIND sono la 8 e la 9. L'Internet Systems Consortium raccomanda a tutti gli utenti di BIND di migrare al più presto possibile la versione 9.
- I server DNS sono integrati in molti prodotti comuni quali firewall, server di rete e security appliances. Tutti i server, gli appliances e i sistemi che si affacciano a Internet devono essere controllati per verificare che qualsiasi software DNS incluso sia stato aggiornato e configurato seguendo le raccomandazioni del fornitore.
- I server che non sono destinati specificamente a supportare transazioni DNS (ad esempio i mail server, i file server o i web server) non devono eseguire una applicazione o un demone DNS a meno che ciò non sia assolutamente necessario.

C6.6 Riferimenti

Vulnerabilità DNS

<http://www.sans.org/newsletters/risk/display.php?v=4&i=11>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=14#widely1>

<http://isc.sans.org/presentations/dnspoisoning.php>

<http://thekelleys.org.uk/dnsmasq/doc.html>

<http://www.icir.org/vern/papers/reflectors.CCR.01/node8.html>

Sondaggio sulle versioni DNS e Server Software

<http://mydns.bboy.net/survey/>

<http://www.dns.net/dnsrd/servers/>

Funzionamenti interni di DNS

<http://www.internic.net/faqs/authoritative-dns.html>

<http://www.sans.org/rr/whitepapers/dns/>

<http://www.cert.org/archive/pdf/dns.pdf>

<http://www.isc.org/index.pl>

<http://www.microsoft.com/windows2000/technologies/communications/dns/default.mspx>

<http://www.dns.net/dnsrd/>

Implementazione di DNSSEC

<http://www.dnssec-deployment.org/>

<http://www.dnssec.net>

<http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf>

Best Practice per la sicurezza dei DNS

<http://www.cymru.com/Documents/secure-bind-template.html>

<http://www.softpanorama.org/DNS/security.shtml>

http://cookbook.linuxsecurity.com/sp/bind_hardening8.html

<http://www.isc.org/index.pl?sw/bind/bind-security.php>

http://www.cisecurity.org/bench_bind.html

http://www.cert.org/tech_tips/usc20_full.html

C7. Software di Backup

C7.1 Descrizione

Il software di backup è un bene prezioso per qualsiasi organizzazione. Di solito questi software agiscono su un gran numero di sistemi di ciascuna azienda. Negli ultimi anni, con la crescita della quantità di dati gestiti, la tendenza è stata quella di consolidare la funzione di backup in pochi server, o anche in un unico server dedicato. Di conseguenza i singoli host che necessitano del servizio di backup comunicano con il server di backup attraverso la rete. Ciò può avvenire in modalità *push* quando il client invia i dati al server o in modalità *pull* quando è il server a connettersi a sua volta con ciascun client, o in una combinazione di queste due modalità. Nell'ultimo anno sono state scoperte diverse vulnerabilità critiche nei software di backup. Queste vulnerabilità possono essere sfruttate per ottenere il controllo completo dei sistemi che ospitano i server di backup e/o i client di backup. Un aggressore può far leva su questi difetti del software per compromettere tutti i sistemi aziendali e per ottenere l'accesso a dati riservati presenti nei backup. Alcuni exploit sono stati pubblicati in rete e molte vulnerabilità sono state attaccate in maniera selvaggia.

C7.2 Sistemi operativi e software di Backup interessati

Tutti i sistemi operativi su cui operano i software per server o client di backup sono potenzialmente vulnerabili agli exploit. I sistemi operativi interessati sono principalmente sistemi Windows e UNIX.

I seguenti pacchetti software di backup molto diffusi sono affetti da vulnerabilità

- Symantec Veritas NetBackup/Backup Exec
- Computer Associates BrightStor ARCserve
- EMC Legato Networker

C7.3 Voci CVE

[CVE-2005-3116](#), [CAN-2005-3659](#), [CAN-2005-3658](#), [CVE-2006-0989](#), [CVE-2006-0990](#), [CVE-2006-0991](#), [CVE-2006-5142](#), [CVE-2006-5143](#)

C7.4 Come stabilire se si è vulnerabili

- Usate un vulnerability scanner per scoprire le eventuali vulnerabilità del software di backup.
- Se usate uno dei software di backup menzionato sopra, vi raccomandiamo di aggiornarlo alla versione più recente. Controllate periodicamente il sito del produttore del software e iscrivetevi al sistema di notifica delle patch, se disponibile. Controllate anche nei siti dedicati alla sicurezza come [US-CERT](#), [CERT](#), [SANS \(Internet Storm Center\)](#) se vi sono annunci relativi a vulnerabilità legate al software di backup che avete scelto.
- Le porte normalmente utilizzate dal software di backup sono:
 - o Symantec Veritas Backup Exec -TCP/10000 TCP/8099, TCP/6106, TCP/13701, TCP/13721 e TCP/13724 (Una lista delle porte utilizzate dai daemon di backup di Veritas è disponibile [qui](#))
 - o CA BrightStor ARCserve Backup Agent -TCP/6050, UDP/6051, TCP/6070, TCP/6503, TCP/41523, UDP/41524
 - o Sun e EMC Legato Networker -TCP/7937-9936

C7.5 Come proteggersi da queste vulnerabilità

- Assicuratevi che le patch più recenti fornite dal produttore del software sia installate sui client e sui server.

- Le porte utilizzate dal software di backup dovrebbero essere protette tramite regole dei firewall dall'utilizzo tramite qualsiasi rete non sicura, inclusa Internet.
- I dati dovrebbero essere cifrati sia quando sono salvati sui supporti di backup, sia quando transitano attraverso la rete.
- I firewall di rete e relativi al singolo host dovrebbero presentare regole che limitano l'accessibilità ai sistemi su cui operano i software di backup in modo che solo l'host di backup corretto possa comunicare attraverso le porte del server di backup.
- Suddividete la vostra rete creando una sottorete VLAN separata per il backup.
- I supporti di backup dovrebbero essere conservati, tracciati e contabilizzati come gli altri asset IT per scoraggiare e individuare prontamente il furto o la perdita.
- I supporti di backup dovrebbero essere cancellati in modo sicuro o distrutti fisicamente alla fine del loro periodo di utilizzo.

C7.6 Riferimenti

Consigli Computer Associates

<http://supportconnectw.ca.com/public/storage/infodocs/basbr-secnotice.asp>

<http://zerodayinitiative.com/advisories/ZDI-06-030.html>

<http://zerodayinitiative.com/advisories/ZDI-06-031.html>

Consigli Symantec Veritas

<http://seer.support.veritas.com/docs/279553.htm>

<http://support.veritas.com/docs/281521>

<http://www.idefense.com/application/poi/display?id=336&type=vulnerabilities>

<http://www.zerodayinitiative.com/advisories/ZDI-06-005.html>

<http://www.zerodayinitiative.com/advisories/ZDI-06-006.html>

Consigli EMC Legato e Sun

http://www.legato.com/support/websupport/product_alerts/011606_NW.htm

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0027.html>

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0028.html>

<http://archives.neohapsis.com/archives/vulnwatch/2006-q1/0029.html>

C8. Directory Server, sistemi di monitoraggio e per la gestione della sicurezza

C8.1 Descrizione

Applicazioni server come i sistemi antivirus e antispam, di directory server e i sistemi di gestione e monitoraggio rappresentano una particolare sfida per la sicurezza; oltre a compromettere i sistemi che li ospitano, forniscono l'opportunità di attaccare altri sistemi.

C8.2 Applicazioni colpite

Le applicazioni interessate al problema possono essere suddivise in diverse categorie:

- **Directory Server** – Utilizzati per gestire informazioni riguardanti gli utenti e i sistemi. Compromettere queste applicazioni può consentire l'accesso a grandi quantità di informazioni, compresi gli username e le password (possibilmente crittate).
- **Sistemi di monitoraggio** – Utilizzati per monitorare altri sistemi di vario tipo. Queste applicazioni spesso possiedono degli account sui sistemi monitorati, consentendo agli aggressori di accedere facilmente a tali sistemi.

- **Sistemi per l'aggiornamento di configurazioni e patch** – Questi sistemi sono utilizzati per gestire le configurazioni e le patch dei client. Compromettere questi sistemi offre una via privilegiata per la diffusione di malware.
- **Sistemi antivirus e antispyware** – Le vulnerabilità in questi sistemi possono spesso essere sfruttate con interazioni dell'utente minime o nulle, inviando semplicemente un messaggio email appositamente predisposto. Una volta compromesso il sistema, l'aggressore può inviare più facilmente email che contengono spam o virus. Inoltre questi sistemi spesso contengono informazioni critiche, come la casella di posta degli utenti.

Queste applicazioni operano su diversi sistemi operativi, da Microsoft Windows a Solaris o, più raramente, HP-UX e Novell Netware.

C8.3 Voci CVE

[CVE-2006-5478](#), [CVE-2006-4509](#), [CVE-2006-4510](#), [CVE-2006-4177](#), [CVE-2006-2496](#), [CVE-2006-0992](#), [CVE-2005-3653](#), [CVE-2005-1928](#), [CVE-2005-1929](#)

C8.4 Come stabilire se si è a rischio

- Utilizzando un vulnerability scanner.
- Controllando gli avvisi di sicurezza del fornitore.

C8.5 Come proteggersi da queste vulnerabilità

- Mantenendo i sistemi aggiornati con le patch e i service pack più recenti. Se disponibile, utilizzate un sistema automatizzato.
- Utilizzando sistemi di Intrusion Prevention/Detection per prevenire/individuare attacchi che utilizzano queste vulnerabilità.
- Controllando che solo gli utenti e i sistemi autorizzati abbiano accesso ai sistemi a rischio.

C8.6 Riferimenti

Vulnerabilità di ServerProtect Trend Micro

<http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0066.html>

<http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0067.html>

<http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0068.html>

Home Page di Trend Micro

<http://www.trendmicro.com/>

Buffer Overflow in iTechnology iGateway CA

http://supportconnectw.ca.com/public/ca_common_docs/igatewaysecurity_notice.asp

Home Page CA

<http://www.ca.com/>

Buffer Overflow remoto in Novell eDirectory iMonitor

<http://www.zerodayinitiative.com/advisories/ZDI-06-016.html>

Home Page Novell

<http://www.novell.com>

SQL Injection in Sygate Management Server Symantec

<http://securityresponse.symantec.com/avcenter/security/Content/2006.02.01.html>

Home Page Symantec

<http://www.symantec.com/>

Esecuzione di comandi da remoto in OpenView HP

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00672314>

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00671912>

Esecuzione di codice da remoto in OpenView Storage Data Protector HP

<http://archives.neohapsis.com/archives/bugtraq/2006-08/0273.html>

Home Page di OpenView HP

<http://h20229.www2.hp.com/>

Vulnerabilità in Update Server PatchLink

<http://archives.neohapsis.com/archives/bugtraq/2006-06/0631.html>

Home Page di PatchLink

<http://www.patchlink.com/>

Remote Command Injection in Spam Firewall Barracuda

<http://archives.neohapsis.com/archives/bugtraq/2006-08/0093.html>

Home Page Barracuda

<http://www.barracudanetworks.com/ns/?L=en>

Buffer Overflow remoto in ePolicy Orchestrator/ProtectionPilot McAfee (McAfee Home Page)

<http://www.mcafee.com/>

N1 Server e telefoni VoIP

N1.1 Descrizione

L'utilizzo delle tecnologie VoIP ha continuato a diffondersi anche corso dell'anno appena concluso. Nello stesso tempo, c'è stato un incremento nel controllo della sicurezza per i tipici componenti delle reti VoIP, come i call proxy, i media server e gli stessi telefoni VoIP. Sono stati individuate vulnerabilità che possono portare a un crash o a un completo controllo sfruttando le vulnerabilità del server o del dispositivo anche in prodotti come Cisco Unified Call Manager, Asterisk e in telefoni VoIP di vari fornitori. Quando arriva a controllare i server o i telefoni IP, un aggressore può usarli per veicolare attacchi di phishing VoIP, di eavesdropping, di frodi tariffarie o di denial-of-service.

Siccome molti server VoIP - specialmente quelli presso i service provider VoIP - sono una interfaccia tra SS7 (la segnalazione telefonica tradizionale) e le reti IP, un attaccante in grado di compromettere uno server VoIP vulnerabile potrebbe potenzialmente manipolare la segnalazione SS7 e interrompere i servizi di interconnessione per la Public Switched Telephone Network (PSTN), ovvero la tradizionale linea telefonica.

N1.2 Voci CVE

Asterisk

[CVE-2006-2898](#), [CVE-2006-4345](#), [CVE-2006-4346](#), [CVE-2006-5444](#)

Cisco Call Manager

[CVE-2006-0368](#), [CVE-2006-3594](#)

Telefoni VoIP

[CVE-2005-3717](#), [CVE-2005-3722](#), [CVE-2005-3723](#), [CVE-2006-0305](#), [CVE-2006-0374](#), [CVE-2006-0834](#), [CVE-2006-5038](#)

N1.3 Come mitigare queste vulnerabilità VoIP

- Applicare le patch fornite dal produttore ai server VoIP e al software/firmware del telefono non appena queste diventano disponibili.

- Assicuratevi che i sistemi operativi che girano sui server VoIP abbia installate le patch più recenti, sia quelle rilasciate dal produttore del sistema operativo, sia quelle del prodotto VoIP.
- Effettuate scansioni del server e dei telefoni VoIP per rilevare le porte aperte. Nel firewall chiudete l'accesso da Internet a tutte le porte non necessarie alle operazioni dell'infrastruttura VoIP.
- Utilizzare un firewall che gestisca il protocollo VoIP o un prodotto di Intrusion Prevention per controllare che tutte le porte UDP sui telefoni VoIP non siano aperte alle comunicazioni internet RTP/RTCP.
- Disabilitate sui telefoni e sui server tutti i servizi non indispensabili (telnet, http ecc.)
- Considerate per i vari componenti VoIP l'uso di strumenti specifici come [OULU SIP PROTOS Suite](#) per garantire l'integrità dello stack del protocollo VoIP.
- Nella fase di selezione del prodotto, prestate molta attenzione alle tempistica con la quale i fornitori di prodotti VoIP rilasciano le patch necessarie al sistema operativo non appena queste sono disponibili. Numerosi produttori di VoIP rilasciano patch non ufficiali, che richiedono parecchio tempo prima della loro approvazione.
- Usate VLAN separate per la vostra rete dati e la rete voce, se la vostra infrastruttura di rete lo permette. Controllate che i server TFTP e DHCP VoIP siano separati dalla vostra rete dati.
- Cambiate la password di default per il login nel pannello di amministrazione di telefoni e proxy.

N1.4 Riferimenti

Vulnerabilità di Asterisk

<http://www.asterisk.org/>

<http://archives.neohapsis.com/archives/bugtraq/2006-06/0139.html>

<http://archives.neohapsis.com/archives/fulldisclosure/2006-08/0617.html>

<http://archives.neohapsis.com/archives/bugtraq/2006-10/0311.html>

Vulnerabilità di Cisco Unified Call Manager

http://www.cisco.com/en/US/products/products_security_advisory09186a00805e8a55.shtml

General VoIP Security Information VoIPSA Organization

<http://www.voipsa.org>

NIST Considerazioni sulla sicurezza dei sistemi VoIP

<http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>

N2. Debolezze diffuse nella configurazione dei dispositivi di rete

N2.1 Descrizione

I dispositivi di rete, come router e switch, spesso godono di una reputazione di sicurezza e la stabilità. Anche i dispositivi accessibili via rete, come stampanti e fax, sono spesso considerati intrinsecamente sicuri. Molto spesso, invece, per entrambe le classi di dispositivi mancano politiche e verifiche di sicurezza.

Per il ruolo particolare che questi dispositivi svolgono nell'infrastruttura di rete, spesso si adottano configurazioni predefinite che privilegiano la facilità d'uso e di configurazione, piuttosto che la sicurezza. In questa sezione verranno affrontati i problemi di sicurezza più diffusi presenti in molte configurazioni di default di dispositivi di rete o accessibili via rete.

N2.2 Problemi comuni delle configurazioni predefinite

N2.2.1 Community String SNMP predefinite.

Community string di default e, spesso, community string hard-coded continuano ad essere un problema per i prodotti di rete. Quest'anno Cisco IOS, nelle versioni dalla 12.2 alla 12.4 fino alla release 20060920,

utilizzate da alcuni dispositivi Cisco e da uno switch 3Com, è risultato vulnerabile a questo problema. Esempi CVE: [CVE-2006-4950](#), [CVE-2006-5382](#)

N2.2.2 Impostazioni di default per account, password, chiavi di crittografia e token.

Molti dispositivi sono configurati con password di default e di altri token di autenticazione predefiniti che, spesso, consentono l'accesso amministrativo completo al dispositivo. Nel caso di dispositivi wireless, le chiavi crittografiche predefinite possono consentire di monitorare e intercettare facilmente il traffico.

Esempi CVE: [CVE-2006-0789](#), [CVE-2006-0834](#), [CVE-2006-3287](#).

N2.2.3 Servizi non necessari

Molti dispositivi sono configurati per l'esecuzione di altri servizi oltre a quelli necessari per l'attività affidata al dispositivo. Ad esempio, molte stampanti forniscono interfacce di stampa HTTP e FTP. Queste interfacce sono spesso abilitate per default. I servizi non necessari rappresentano potenziali buchi di sicurezza, e rendono più complicata la connessione e l'amministrazione del dispositivo.

N2.2.4 Protocolli di amministrazione non autenticati e in chiaro

I dispositivi sono spesso gestiti tramite protocolli che non supportano la crittografia o l'autenticazione. Le interfacce di amministrazione HTTP e telnet trasmettono tutte le informazioni in chiaro, TFTP trasmette tutte le informazioni in chiaro e non supporta l'autenticazione. Dove possibile, si dovrebbero usare protocolli che prevedono crittografia e autenticazione, come HTTPS e SCP.

N2.3 Vulnerabilità delle stampanti

Dispositivi come stampanti, fax e scanner spesso contengono i problemi di configurazione descritti precedentemente. Questi dispositivi operano spesso privi delle necessarie patch e possono rappresentare un notevole rischio di sicurezza per una organizzazione.

Esempi CVE: [CVE-2006-0788](#), [CVE-2006-2108](#)

N2.4 Come proteggersi da queste vulnerabilità

N2.4.1 Effettuate un controllo completo della configurazione

Salvare le configurazioni dei dispositivi in un archivio centralizzato e controllare regolarmente queste configurazioni può semplificare l'individuazione di eventuali punti deboli.

Un possibile aiuto nella gestione delle configurazioni sono anche strumenti come Cisco CiscoWorks di Cisco.

Home Page di CiscoWorks <http://www.cisco.com/en/US/products/sw/cscowork/ps2425/>

RANCID –Cisco Config Monitoring Tool <http://www.shrubbery.net/rancid>

CISecurity Network Element Benchmarks and Audit Tools <http://www.cisecurity.org>

N2.4.2 Implementate un server syslog

Molti dispositivi supportano la connessione tramite il protocollo syslog. I server syslog sono inclusi per default su tutti i sistemi Unix, o tipo Unix, e Linux. Anche per Microsoft Windows sono disponibili dei server syslog gratuiti. Configurando correttamente i log su un dispositivo di rete, si permetterà al server syslog di registrare gli accessi al dispositivo, nonché qualsiasi modifica alla configurazione come le eventuali violazioni delle norme applicate al dispositivo.

Configurare Cisco Syslog <http://www.linuxhomenetworking.com/cisco-hn/syslog-cisco.htm>

Central Loghost Mini-HOWTO <http://www.campin.net/newlogcheck.html>

N2.4.3 Disattivate gli account predefiniti e cambiate le password di default

Qualsiasi account predefinito dovrebbe essere disattivato e tutte le password di default (e altri token di autenticazione) dovrebbero essere sostituite con altre più sicure.

Cisco SNMP Community Strings

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

N2.4.5 Usate protocolli di amministrazione autenticati e crittati

Se il dispositivo supporta l'amministrazione tramite HTTPS o SSH, questi protocolli sono da preferire rispetto a quelli in chiaro come HTTP o telnet. Per il trasferimento di file, SCP, HTTPS o FTPS sono da preferire a TFTP o FTP. Si dovrebbe inoltre utilizzare password robuste o altri metodi di autenticazione.

Configurare SSH su dispositivi Cisco

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html

N2.4.6 Utilizzare Port-Level Security

se la vostra infrastruttura di rete la supporta, adottate sugli switch la port-level security. Questa opzione può aiutare a prevenire il collegamento alla rete di sistemi non autorizzati e può contribuire a contenere e individuare spoofing ARP e altri attacchi.

H1. Diritti eccessivi dell'utente e dispositivi non autorizzati

H1.1 Introduzione

Alcuni attacchi non possono essere efficacemente prevenuti dai soli controlli tecnici. Gli utenti imprudenti possono essere attratti verso operazioni poco sicure. Gli utenti più smaliziati possono inventare metodi poco sicuri di eseguire alcuni compiti, esponendo involontariamente i loro datori di lavoro a molti rischi. Per prevenire che tali rischi siano sfruttati da attacchi sono necessari controlli organizzativi per completare i controlli tecnici e fisici.

Col passare del tempo, i controlli tecnici possono essere in grado di applicare politiche che precludono alcuni comportamenti degli utenti, ma fino a quando questo risultato non viene raggiunto sono importanti dei controlli periodici al fine di garantire che i controlli organizzativi siano efficaci. È inoltre essenziale istituire un processo rilevare le violazioni alle politiche scelte e garantire che eventuali sistemi non conformi siano riportati a una situazione di rispetto delle politiche scelte in modo efficace.

H.1a Dispositivi infetti e/o non autorizzati in rete

I migliori sforzi per garantire la sicurezza di un sistema informatico diventano inutili se gli utenti connettono dispositivi non autorizzati alla rete o a un computer. Una access point wireless non autorizzato può essere una porta aperta a qualsiasi malintenzionato che vogliono avere un accesso alla rete. Un computer portatile collegato a una rete aziendale può introdurre qualsiasi malware, infettando l'intera rete. I laptop aziendali non protetti che siano stati collegati a reti pubbliche poco sicure possono trasmettere tutti i malware raccolti e condividerli con l'intera organizzazione. Un router o un PC connessi senza autorizzazione da un visitatore attraverso una porta ethernet aperta, possono aprirgli una porta privilegiata verso l'intera rete aziendale. Una chiavetta USB contenente un virus può infettare un PC semplicemente se inserita nella porta.

Nello stesso tempo, gli amministratori di rete dovrebbero fare attenzione agli utenti che ritornano dopo essersi connessi ad altre reti. Le policy di sicurezza dovrebbero indicare quali sono gli utenti autorizzati a fare ciò, ma le verifiche e un controllo degli accessi in rete possono assicurare che le politiche di sicurezza siano state seguite.

Un continuo monitoraggio del flusso dei dati può rivelare immediatamente dispositivi non autorizzati. Un sistema di controllo degli accessi in rete può inoltre effettuare una scansione sui computer aziendali per individuare virus, trojan, spyware e adware, rilevando le vulnerabilità nascoste portate in rete da fuori. È possibile quindi isolare i sistemi vulnerabili e correggere il problema, e quindi assegnare loro i diritti di accesso appropriati.

H.1b Diritti eccessivi dell'utente e software non autorizzato

Il software non regolamentato introduce in azienda diversi rischi. Tale software può contenere vulnerabilità di sicurezza e chi lo usa può non essere sufficientemente informato o motivato per applicare regolarmente le patch. Inoltre gli utenti possono installare software che, senza che gli utenti lo sappiano, contiene malware che potrebbero portare a compromettere la sicurezza dei dati o della rete. Gli utenti potrebbero anche installare software che forniscono funzionalità tali (ad esempio il file sharing peer-to-peer) da introdurre nuove vulnerabilità nell'ambiente di rete. Chi è responsabile per la sicurezza delle informazioni dovrebbe quindi prendere in considerazione l'attuazione di politiche, e dei corrispondenti controlli correttivi, atte a mitigare tali vulnerabilità.

Si è vulnerabili se gli utenti possono installare autonomamente software e non sono state adottate contromisure adeguate per controllare questo processo.

La contromisura da adottare per prevenire un problema di questo tipo consiste nell'istituire una politica di sicurezza capace di limitare i diritti degli utenti. Se un utente può installare software senza autorizzazione, anche i malware presenti sul sistema possono installare software. Per limitare questo problema è utile anche mantenere delle liste di software autorizzati, come controllare tutti i sistemi quando si connettono alla rete per verificare che non sia presente software non autorizzato.

H1.2 Riferimenti

<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17170&TEMPLATE=/ContentManagement/ContentDisplay.cfm>

http://www.techweb.com/wire/security/20020904_security

<http://technet2.microsoft.com/WindowsServer/en/library/e903f7a2-4def-4f5f-9480-41de6010fd291033.mspx?mfr=true>

http://www.sans.org/resources/policies/Password_Policy.pdf

http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

<http://www.cerias.purdue.edu/weblogs/spaf/general/post-30/>

<http://www.csoonline.com/caveat/062306.html>

H2. Utenti (Phishing e Spear Phishing)

H2.1 Descrizione

La parola "phishing" fu usata la prima volta quando nel 1996 alcuni hacker iniziarono a impadronirsi di account di America On-Line inviando messaggi e-mail agli utenti AOL che fingevano di provenire dalla stessa America On-Line. Gli attacchi di phishing oggi prendono di mira utenti di servizi di online banking, di servizi di pagamento come PayPal e di siti di commercio elettronico. Questi attacchi sono rapidamente cresciuti in numero e in sofisticatezza. Fin dall'agosto 2003, le maggiori banche USA, del Regno Unito e dell'Australia sono infatti state vittime di attacchi phishing.

Password/PIN Phishing

Gli autori del phishing inviano email ad utenti proprietari di un conto on line al fine di indirizzarli verso un sito internet istituito ad hoc, dove con l'inganno vengono loro carpite informazioni che consentono loro di sottrarre il denaro presente sul conto. Questa tecnica viene anche utilizzata per ottenere informazioni relative ad account online come quelli di Hotmail, Yahoo ed eBay. Una volta entrati in possesso di username e password, i phisher tenteranno di procurarsi le informazioni relative ai conti della vittima. Se un individuo si impossessa dell'account di eBay, ad esempio, ha facilmente accesso a tutte le transazioni correnti e passate effettuate dalla vittima, informazioni personali come i dati relativi a i pagamenti con Paypal, nonché l'indirizzo fisico della vittima.

VoIP phishing

Una nuova forma di phishing sostituisce il sito web con un numero di telefono. In questa tecnica di phishing, una e-mail vi invita a chiamare uno specifico numero dove un sistema di risposta automatica, installato presso una linea telefonica VoIP compromessa, è in attesa di prendere il vostro numero di conto, numeri di identificazione personale, password o altri dati personali di valore. Se vi rifiutate di rispondere alle domande della persona o del sistema audio dall'altra parte del filo, vi racconteranno che il vostro conto verrà chiuso o si potrebbero verificare altri problemi simili.

Spear Phishing

Lo Spear phishing è un attacco di phishing molto mirato. Gli autori di questo tipo di frode inviano messaggi di posta elettronica che contengono informazioni che riguardano gli impiegati o problemi organizzativi correnti dell'azienda, che quindi fanno apparire i messaggi attendibili a tutti gli impiegati o i membri di una determinata azienda, ente pubblico, organizzazione o gruppo. Il messaggio può apparire come inviato dal datore di lavoro o da un collega che avrebbe potuto spedire un messaggio e-mail a tutto il personale, come ad esempio il responsabile delle risorse umane o colui che gestisce il sistema informativo, e può comprendere richieste legate a username o password. Lo spear phishing è diventato una delle forme di attacco più devastanti presso le organizzazioni militari americane e di altri paesi sviluppati. I phisher guadagnano in questo modo informazioni sugli username e sulle password che utilizzano per intrufolarsi attraverso i sistemi di filtro che proteggono le informazioni militari riservate.

H2.1 Come prevenire gli attacchi di phishing

Uno dei metodi più promettenti per fermare lo spear phishing consiste nel programmare periodicamente per tutti gli utenti degli esercizi attraverso i quali sperimentare del phishing inoffensivo. Un bimbo spesso impara a non toccare una stufa dopo che si è bruciato le dita. Facendo un'esperienza di phishing illuminante, ma non pericolosa, si può ottenere lo stesso effetto senza fare danni reali.

Un secondo metodo di difesa consiste in un metodo di autenticazione a due fattori. Se l'organizzazione non è economicamente forte e non può permettersi un metodo di autenticazione a due fattori, un altro metodo utilizzato per prevenire il phishing e altri tipologie di problemi consiste nell'utilizzo di strumenti di verifica come immagini segrete o domande di conferma. I sistemi a immagine segreta (Secret Images) si basano sulla scelta preventiva da parte di un utente di una o più immagini. Le immagini sono conosciute solo dal cliente e dal sistema che lo deve autenticare: il processo mostra all'utente queste immagini e l'utente è istruito sul fatto che se il sito non presenta l'immagine corretta significa che NON è un sito legittimo e che deve contattare al più presto possibile il supporto clienti. Le domande di conferma (Challenge Questions) funzionano in modo simile: l'utente ha preventivamente concordato una serie di domande e risposte, note solo al cliente e al sistema di autenticazione. Quando deve autenticarsi, all'utente sono poste una o più di queste domande al quale deve rispondere nella maniera concordata.

Metodi meno efficaci, ma comunque validi sono:

- Evitare di inviare mail comuni ai vostri clienti con link diretti al vostro sito web o a un sito terzo. In questo modo si abitua i clienti ad accettare e-mail che aprono dei link web e a ritenerle affidabili. Ciò vi esporrà in futuro ad attacchi phishing.
- Non usate le vostre credenziali di autenticazione o altre informazioni personali non pubbliche (es. pin del bancomat, codice fiscale ecc. usati come password per il vostro portale web) per autenticare la vostra clientela.
- Inserite nei log informazioni come l'indirizzo IP, informazioni di localizzazione e sistemi di riconoscimento dei computer per tracciare qualsiasi dispositivo che acceda online e modifichi i dati degli utenti.
- Assicuratevi che tutti i casi di frode siano denunciati all'autorità competente, in modo che le informazioni siano messe in relazione con altri attacchi e vengano studiati in sistemi utilizzati.
- **Anti-Phishing Software:** Nei browser Web e nei client e-mail sono di solito integrate applicazioni che tentano di rilevare contenuti phishing nei messaggi di posta e nei siti Web, presenti anche nei form delle toolbar che mostrano il vero nome di dominio del sito che l'utente sta visitando o sta per visitare, in modo da prevenire attività fraudolente. Ne esistono di diversi tipi, sia come funzione nativa, sia come plug-in per Firefox e per Internet Explorer.
 - [Microsoft IE 7](#)
 - [NetCraft Toolbar](#): disponibile per Internet Explorer e per Firefox
 - [Google Safe browsing](#): disponibile per Firefox
 - [Ebay Toolbar](#): disponibile per Internet Explorer
 - [Earthlink Scamblocker](#): disponibile per Internet Explorer e per Firefox
 - [Geotrust Trustwatch](#) – disponibile per Internet Explorer, Firefox e per [Flock](#)
- **Formazione degli utenti:** una delle migliori strategie per la lotta contro il phishing è quello di educare gli utenti ai metodi correnti e a tutte le nuove tecniche di attacco di phishing, e di renderli edotti su cosa fare in caso di un attacco phishing. Formate i vostri utenti che vengono contattati riguardo il loro account cliente. Istruiteli a contattare la vostra hotline se qualcuno chiede loro da parte vostra qualsiasi informazione personale. Dite agli utenti di digitare ogni volta l'indirizzo del vostro sito nella barra degli indirizzi del browser, in modo da ridurre il rischio che seguano un link contraffatto o fraudolento, specialmente quelli presenti nei messaggi email.
- **Doppia autenticazione (Two Factor Authentication):** Se nessun metodo di prevenzione è totalmente infallibile è preferibile, per prevenire il phishing o altri tipi di truffe, utilizzare strumenti di verifica come "secret images" o come "challenge questions". Secret images si basa sulla scelta anticipata da parte di un utente di una o più immagini. Le immagini sono conosciute solamente dal cliente e da chi lo deve autenticare. Se l'utilizzatore finale non visualizza nel sito una di queste immagini, comprende che il sito non è legittimo e contatta il servizio clienti il più rapidamente possibile. Challenge questions invece si basa sulla selezione, da parte dell'utente, di un serie domande riservate di cui sono a conoscenza solamente il cliente e da chi lo deve autenticare. Quando deve autenticarsi, all'utente sono poste una o più di queste domande al quale deve rispondere nella maniera concordata.

H2.2 Riferimenti:

AntiPhishing Working Group

<http://www.antiphishing.org/>

<http://www.3sharp.com/projects/antiphishing/gonephishing.pdf>

VoIP Phishing Scams

<http://blogs.pcworld.com/staffblog/archives/001921.html>

Z1: Sezione speciale: Attacchi Zero Day e strategie di prevenzione

Z1.1 Descrizione

Per quanto i rischi e lo sfruttamento delle vulnerabilità Zero Day nelle più diffuse applicazioni fossero già noti da numerosi anni, gli attacchi Zero Day effettuati nel 2006 hanno fatto segnare un incremento significativo rispetto al periodo precedente. Una vulnerabilità zero day si verifica quando un difetto nel codice nel software viene scoperto e sfruttato prima che sia disponibile una patch o una soluzione. Una volta diffuso un exploit che sfrutta queste vulnerabilità, gli utenti del software interessato sono inermi fino a quando non è disponibile una patch o fino a quando non viene adottata una qualche forma di contromisura da parte dell'utente. I passi da seguire per mitigare il pericolo e proteggersi da tale minaccia verranno indicati nel corso di questa sezione.

Z1.2. Sistemi operativi interessati

Per tutti i sistemi operativi e per tutte le applicazioni software è possibile scoprire ed eventualmente sfruttare una vulnerabilità zero day. Anche se la maggior parte degli attacchi di quest'anno sono stati diretti contro prodotti Microsoft, anche Apple è stata colpita da diversi exploit zero day. Non sono stati invece registrati attacchi zero day verso Linux, BSD o su altri sistemi operativi basati su Unix.

Z1.3. Voci CVE

Lo scorso anno numerose vulnerabilità sono state sfruttate prima che fosse messa in circolazione una patch ufficiale o studiato un rimedio. Alcuni esempi di voci CVE che riflettono questa tendenza sono:

- Windows Graphical Device Interface Library (.wmf) [CVE-2005-4560](#)
- Microsoft Internet Explorer [CVE-2006-1245](#)
- Microsoft Internet Explorer [CVE-2006-1359](#)
- Microsoft Internet Explorer [CVE-2006-1388](#)
- Microsoft Internet Explorer [CVE-2006-3280](#)
- Microsoft Internet Explorer [CVE-2006-3281](#)
- Microsoft Internet Explorer [CVE-2006-4777](#)
- Apple OS X [CVE-2006-1982](#)
- Apple OS X [CVE-2006-1983](#)
- Apple Safari [CVE-2006-1986](#)
- Apple Safari [CVE-2006-1987](#)
- Microsoft Word [CVE-2006-2492](#)
- Microsoft Excel [CVE-2006-3086](#)
- Microsoft PowerPoint [CVE-2006-3590](#)
- Microsoft PowerPoint [CVE-2006-4694](#)
- Microsoft PowerPoint [CVE-2006-5296](#)
- Microsoft Windows Help File Viewer [CVE-2006-4138](#)
- Microsoft Internet Explorer and Outlook [CVE-2006-4868](#)

- Microsoft Visual Studio [CVE-2006-4704](#)
- Microsoft XML HTTP ActiveX [CVE-2006-5745](#)

Z1.4. Come proteggersi da queste vulnerabilità

La protezione contro lo sfruttamento delle vulnerabilità zero day è una questione di grande preoccupazione per la maggior parte degli amministratori di sistema. Per ridurre la pericolosità degli attacchi zero day, è opportuno seguire alcune *best practice* quali:

- Adottare una posizione *deny-all* sui firewall e sui dispositivi perimetrali che proteggono le reti interne
- Separare i server con affaccio pubblico dai sistemi interni
- Disattivare i servizi non necessari e rimuovere le applicazioni che non siano richieste da esigenze operative
- Seguire il principio del minimo privilegio possibile nell'impostazione dei controlli di accesso, dei permessi e dei diritti degli utenti
- Impedire o limitare nei browser l'uso di codice attivo come Java script o ActiveX
- Sensibilizzare gli utenti in merito ai rischi connessi all'apertura di file allegati non richiesti
- Disabilitate la possibilità di seguire i link presenti nei messaggi di posta elettronica
- Disabilitate la possibilità di scaricare automaticamente le immagini da Web nei messaggi di posta elettronica
- Gestire internamente (o, se necessario affidare all'esterno) un servizio di gestione degli allarmi e degli avvisi di sicurezza rapido ed efficiente per essere certi di venire a conoscenza degli exploit zero-day exploit non appena diventano pubblici
- Utilizzare soluzioni di gestione end-point per rendere più rapida la distribuzione di patch o di soluzioni alternative appena queste si rendono disponibili
- Qualora si utilizzi Microsoft Active Directory, trarre il massimo vantaggio dai Group Policy Objects per controllare gli accessi degli utenti
- Non fare affidamento esclusivamente sulla protezione di un antivirus, in quanto gli attacchi zero-day spesso non si possono scoprire fino a quando non vengono rilasciate le nuove firme
- Quando possibile, utilizzare su tutti i sistemi protezioni da buffer overflow di terze parti
- Seguire le raccomandazioni dei produttori sulle soluzioni alternative e sulle strategie per la riduzione del rischio fino a quando diventa disponibile una patch

Hanno collaborato alla versione italiana della Top-20 2006

- Luca Springolo, Data Security
- Simone Brun, Data Security

Gli esperti che hanno contribuito alla lista Top-20 2006

- Project Manager and Editor: Rohit Dhamankar, TippingPoint, a division of 3Com
- Adam Safier, Global Systems & Strategies, Inc.
- Alan Rouse, Security Architect, TANDBERG Television
- Alexander Kotkov, UBS Investment Bank
- Amol Sarwate, Manager of Vulnerability Lab, Qualys
- Andrew van der Stock, Director, OWASP
- Anton Chuvakin, Director of Product Management @ LogLogic
- Anthony Richardson, Monash University, Australia
- Arturo "Buanzo" Busleiman -Consultor Independiente en Seguridad, Argentina

- Cesar Tascon Alvarez, Ernst and Young, Spain
- Christopher Bream, PricewaterhouseCoopers
- Chris Riley, Spherion
- Christopher Rowe, Guilford Technical Community College
- Ed Fisher, Ingersoll Rand
- Gerhard Eschelbeck, CTO, Webroot
- David Damato, PricewaterhouseCoopers
- Donald Smith, Qwest
- Edward Ray, Netsec Design and Consulting
- James King, TippingPoint, a division of 3Com
- Jean-Francois Legault, Deloitte & Touche LLP
- Jeff Pike, Integrated Team Solutions Facility
- John-Thomas Gaietto
- John Tannahill
- Johannes Ullrich, Internet Storm Center, SANS
- Jonathan Rubin, Dominion
- Kevin Hong, Korea Information Security Agency (KISA) and KrCERT/CC
- Koon Yaw Tan, Infocomm Development Authority of Singapore
- Leo Pastor, Advanced Consulting and Training, Argentina and Brazil
- Marcos A. Ferreira Jr., NX Security, Brazil
- Marcus Sachs, SRI International and Internet Storm Center, SANS
- Mark J Cox, RedHat
- Mark Goudie, Data Networking Services, Australia
- Matteo Shea, Senior Security Engineer, Communication Valley S.p.a
- Michel Cusin, Bell Security Solutions, Canada
- Michele Guel, Cisco Systems
- Miguel Guirao, Telcel
- Olivier Devaux, vulnpedia.com
- Pedro Bueno -McAfee AvertLabs
- Rajesh Mony, Webroot
- Ralf Durkee, Security Consultant
- Rhodri Davies, Vistorm, UK
- Richard Bejtlich, Taosecurity
- Rick Wanner, Technical Analyst, Corporate Security, SaskTel
- Robert Baskerville, Vistorm, UK
- Pedro Paulo Ferreira Bueno, Brasil Telecom
- Sandeep Dhameja, Ambiron Trustwave
- Syed Mohamed

Agenzie

- Department of Homeland Security (DHS)
- Computer Emergency Response Team (CERT)
- National Infrastructure Security Coordination Centre (NISCC, UK)
- Computer Emergency Response Team, Canada

FAQ SANS Top-20 2006

Di Rohit Dhamankar, Direttore del progetto

Per chi è stata scritta la lista?

Negli ultimi anni mi è diventato chiaro che la lista SANS Top 20 è utilizzata da organizzazioni molto diverse tra loro. Alcune organizzazioni di grandi dimensioni utilizzano la lista Top-20 per ricontrollare le loro attività intraprese nel miglioramento della sicurezza, mentre alcune organizzazioni più piccole usano questa lista come strumento esclusivo per guidare tutta la loro attività di rimozione e prevenzione delle vulnerabilità. Così, mentre creavamo la lista abbiamo cercato di servire le due diverse platee.

È ancora rilevante, nel 2007, pubblicare un documento con le peggiori vulnerabilità dell'anno?

Alla luce delle considerazioni che seguono, la risposta non può che essere positiva.

- La scansione dei dati su Internet dimostra che ci sono ancora sistemi affacciati su Internet senza le patch per vulnerabilità che sono state ampiamente sfruttate. Personalmente non ho intenzione di smettere di lavorare a questo progetto fino a quando vedrò un qualsiasi worm come Blaster o Slammer generare un evento in un IDS/IPS nella rete di un cliente.
- Anche se tutte le patch fossero applicate, bisognerebbe vederla ancora con le minacce zero-day! La lista di quest'anno include una serie di difese per le minacce zero-day.
- I professionisti della sicurezza sono così concentrati sulla "sfida del giorno" da aver sempre bisogno di promemoria sulle minacce di volta in volta emergenti, in modo che possano cercare risorse per la lotta contro i nuovi pericoli

Perché la lista si chiama Top 20 quando il numero di vulnerabilità attuale (CVE) è di molto superiore a 20?

- La vita potrebbe essere molto più semplice se si potesse creare una lista di 20 voci CVE critiche e poi sostenere che la protezione contro gli attacchi che sfruttano quelle venti vulnerabilità renderebbe Internet sicuro. La realtà, lo sappiamo, è molto diversa. Se solo uno prendesse gli attacchi settimanali alle vulnerabilità delle applicazioni Web rilevate l'anno scorso, vedrebbe che il numero di vulnerabilità critiche è già superiore a 100! Questo è il numero di vulnerabilità che deriva da centinaia di migliaia di tentativi di attacchi sul web ogni giorno. L'approccio della top 20 è quello di aiutare a focalizzare l'attenzione sulle "classi" di vulnerabilità che vengono sfruttate, e fornire una guida per amministratori di sistema, programmatori e manager su come mitigare ciascuna classe di vulnerabilità.
- La Top 20 raggruppa le vulnerabilità critiche in classi in modo che si possano applicare strategie comuni per la protezione di un'intera classe. Per esempio, un largo numero di overflow MS-RPC può essere prevenuto bloccando le porte 139/tcp e 445/tcp sul perimetro di rete.
- La Top 20 aiuta inoltre ad identificare i vettori di diffusione utilizzati da un ampio numero di malware. È triste notare come nel 2006 accada che i malware si diffondano con successo sulle reti usando password identificate con attacchi brute-force!