

Creare e sviluppare applicazioni senza essere amministratori

Marco Russo

Mail: marco@devleap.com

Blog: <http://blogs.devleap.com/marco/>

MCSOFT MCAD MCSE+I MCSA MCDBA MCT

Microsoft Certified
Professional

www.devleap.it

devleap

Agenda

- Perché è giusto farlo
- Vivere senza essere amministratori
- Regole di scrittura
- Sviluppare senza essere amministratori

www.devleap.it

devleap

Perché è giusto farlo

Perché è giusto creare e sviluppare applicazioni senza essere amministratori

www.devleap.it

devleap

I rischi

Azione	Admin	User
Programma in run automatico	SI	PARZ.
Installazione e avviamento servizi	SI	NO
Connessione a server di rete	SI	SI
Installazione keylogger	SI	NO
Invio dati su porte TCP/IP	SI	SI
Installazione driver	SI	NO
Analisi traffico di rete (sniffing)	SI	NO
Controllo remoto PC	SI	PARZ.

PARZ. = Vulnerabilità parziale

www.devleap.it

devleap

Privilegi minimi

- Run with Least Privilege
 - Significa eseguire con il minimo dei privilegi
 - Si applica ad applicazioni Web e Windows
- LPA: Least Privilege Account
 - Utente con privilegi minimi
 - Si applica a un utente che non è amministratore
 - In Windows, un utente che appartiene al gruppo Users di default

www.devleap.it

devleap

Perché è giusto farlo

- Un'applicazione **andrebbe** eseguita con il minimo dei privilegi necessari
 - Limita i danni in caso di errore o attacco
 - Sicurezza, insomma...
- Un'applicazione **dovrebbe essere** eseguibile con il minimo dei privilegi necessari
 - Il programmatore deve pensarci
 - Non tutti i programmatori lo fanno
 - Ecco uno dei motivi per cui i sistemisti ci odiano

www.devleap.it

devleap

Perché è giusto farlo

- **I vantaggi:**
 - **Conseguenze di eventuali virus: limitate**
 - Riduce superficie di attacco
 - **No spyware**
 - Difficile che si installino, non hanno diritti sufficienti
- **Esperimento:**
 - **Un anno di navigazione con un PC senza antivirus, senza anti-spyware e senza firewall**
 - Ma tutti gli aggiornamenti installati tempestivamente
 - Dopo un anno: nessun virus, nessuno spyware
 - **Attenzione: non è una garanzia**, ma aiuta al 95%
 - Si resta **sempre e comunque esposti a vulnerabilità 0day**

www.devleap.it

deVleap

La vostra esperienza

- **Avete mai provato a usare un PC con un utente non amministratore?**
 - Se siete sviluppatori, probabilmente no...
 - Ma io scrivo codice, **ho bisogno** di essere admin!!
- **I vostri programmi sono utilizzabili da LPA?**
 - Se non li avete mai provati così, probabilmente no
- **Cosa bisogna fare per scrivere un programma usabile da LPA?**
 - **Prima di tutto, capire l'esperienza che può provare l'utente...**

www.devleap.it

deVleap

Vivere senza essere amministratori

www.devleap.it

deVleap

L'esperienza da utente

- **Create un logon associato al gruppo Users**
 - No Administrators
 - No Power Users
- **Al logon scoprirete che:**
 - Non potete installare nuove applicazioni
 - Non potete installare plug-in e ActiveX su Internet Explorer
 - Non potete aggiornare le applicazioni esistenti
 - **Alcune applicazioni già installate non si possono più avviare o presentano dei problemi di funzionamento**

www.devleap.it

deVleap

Cos'è che non va?

- **Perché le applicazioni smettono di funzionare:**
 - 60% - Accesso a file/directory non autorizzato
 - 39% - Accesso a Registry non autorizzato
 - <1% - Mancanza di privilegi sufficienti
- **Soluzioni**
 1. **Scrivere meglio il codice...**
 - Ma non sempre si può
 2. **Individuare i problemi e aumentare gli accessi al minimo indispensabile (su file e registry)**
 - Su file e registry, work around fino a nuova versione
 3. **Aumentare i diritti dell'utente**
 - Non è una soluzione, è un tornare al problema

www.devleap.it

deVleap

Guida alla sopravvivenza

- **Il 99% dei problemi è causato da accessi non autorizzati al File System e al Registry**
- **Un tool indispensabile per la diagnosi:**
 - Process Monitor
 - Su www.sysinternals.com

www.devleap.it

deVleap

Problemi di File System

- Directory leggibili da Everyone e modificabili solo da amministratori e power users:
 - C:\
 - C:\WINDOWS
 - C:\WINDOWS\SYSTEM32
 - C:\PROGRAM FILES
- Spesso i programmi aprono in scrittura file in queste directory
 - Anche se poi fanno solo operazioni di lettura
 - Comunque è un errore scrivere in queste directory, ogni utente dovrebbe avere configurazioni separate

www.devleap.it

deVleap

Problemi di Registry

- Hive leggibili da Everyone e modificabili solo da amministratori
 - HKEY_LOCAL_MACHINE
- Spesso i programmi aprono in scrittura queste chiavi di registry
 - Anche se poi fanno solo operazioni di lettura
 - Comunque è un errore scrivere in questa parte di registry, ogni utente dovrebbe avere configurazioni separate e usare HKEY_CURRENT_USER

www.devleap.it

deVleap

Perché tutti questi problemi

- Molti in buona fede
- Windows 9x non ha ACL (Access Control List)
- Tutti gli utenti possono fare tutto (o quasi) su disco e registry
- Le applicazioni sviluppate su Windows 9x funzionano su Windows 2000/XP/2003, ma ignorano l'aspetto della security
- Altre applicazioni non sono state mai testate da utenti non amministratori...

www.devleap.it

deVleap

Regole di scrittura

www.devleap.it

deVleap

4 semplici regole

- Separare dati setup e configurazione utente
- Aprire solo in lettura se si deve leggere
- Accedere a risorse con privilegi minimi
- Memorizzare i dati per utente

www.devleap.it

deVleap

Dati setup e configurazione utente

- Dati setup
 - Informazioni sull'installazione
 - Directory con risorse
 - Impostazioni "globali" come porte TCP/IP per un servizio
 - Configurazione di un servizio
 - Scrivere durante l'installazione su:
 - Registry: hive HKLM (HKEY_LOCAL_MACHINE)
 - C:\Program Files\...

www.devleap.it

deVleap

Dati setup e configurazione utente

- **Configurazione utente (su file)**
 - **Modelli, configurazioni su file (XML o altro):**
C:\Documents and Settings\NOMEUTENTE\Application Data\NOMEAZIENDA\NOMEAPPLICAZIONE\...
 - **Modelli, configurazioni su file (XML o altro) per tutti gli utenti:**
C:\Documents and Settings\All Users\Application Data\NOMEAZIENDA\NOMEAPPLICAZIONE\...
 - Directory in sola lettura per utenti "normali"
 - Ci scrivono solo i gruppi Administrators e Power Users
- **Per ottenere queste directory usare:**
System.Environment.GetFolderPath
 - Vedere parametro Environment.SpecialFolder
 - Molti casi specifici già definiti

www.devleap.it

deVleap

Dati setup e configurazione utente

- **Configurazione utente (su registry)**
 - Configurazione globale (directory con dati, percorsi, impostazioni definite in fase di Setup)
HKEY_LOCAL_MACHINE (abbreviato in **HKLM**)
 - Solo in lettura per utenti "normali"
 - Ci scrive soltanto il gruppo Administrators
 - Configurazione di partenza per tutti gli utenti:
HKEY_USERS\DEFAULT
 - Contenuto copiato nel profilo di un utente al primo logon sulla macchina, non interviene sui profili già esistenti
 - Solo in lettura per utenti "normali"
 - Ci scrive soltanto il gruppo Administrators
 - Configurazione specifica per ogni utente
HKEY_CURRENT_USER (abbreviato in **HKCU**)
 - Diritti completi per l'utente
 - Impossibile vedere la configurazione di un utente diverso (a meno che non si sia Administrators)

www.devleap.it

deVleap

Aprire in sola lettura

- Il setup viene eseguito da un amministratore
 - Crea e modifica qualsiasi file e/o chiave di registry
- Il programma viene eseguito da un utente
- Dopo il setup **accedere solo in lettura** alle informazioni di configurazione
 - Eseguire Open con richiesta diritti sola lettura
 - Effettuare solo operazioni Read
- **Errore comune:**
 - Fare la Open con diritti di lettura e scrittura
 - In seguito, fare solo Read senza fare Write
 - Il problema è che la Open fallisce subito...
 - **Morale: Open va READ ONLY**

www.devleap.it

deVleap

Accedere a risorse con privilegi minimi

- Più in generale, l'accesso a una risorsa va fatto richiedendo privilegi minimi
 - Aprire un file in lettura se non serve scrivere
 - Accedere a processi, thread e semafori senza richiedere diritti più alti del necessario
 - Se si scrive un servizio o un sito web, assegnare un utente con privilegi minimi per accedere alle risorse necessarie al programma
 - Evitare LocalSystem come utente di default
 - Un errore (o un attacco) può essere devastante

www.devleap.it

deVleap

Memorizzare i dati per utente

- I dati dell'utente per default vanno su My Documents
Environment.GetFolderPath(Environment.SpecialFolder.Personal)
 - Diritti di ownership per l'utente
 - Ogni applicazione può vedere "tutti i dati" dell'utente
 - Anche per questo è importante evitare l'installazione di virus e spyware
- Dove mettere dati visibili e modificabili da tutti gli utenti?

www.devleap.it

deVleap

Memorizzare i dati per utente

- Dove mettere dati visibili e modificabili da tutti gli utenti?
 - Non esiste uno standard
 - Problema latente di sicurezza: i dati sono pubblici
 - Esempio: un MDB con la contabilità... non è una buona idea renderlo accessibile a tutti
 - Possibile soluzione:
 - Individuare una directory comune e cambiare le ACL durante il setup (una potrebbe essere **SpecialFolder.CommonApplicationData**)
 - Resta il problema di aggiungere dei nuovi utenti in futuro: deve farlo l'amministratore
 - **NON LASCIARE DIRITTI A EVERYONE!!!**

www.devleap.it

deVleap

Sviluppare senza essere amministratori

www.devleap.it

deVleap

La vita dura dell'utente

- Si può e si deve sviluppare con un utente non amministratore
 - È l'unico modo per capire subito cosa succede ai programmi sviluppati
 - È anche una questione psicologica: vivere sulla propria pelle certe esperienze fa aumentare la sensibilità al problema
 - È un modo più sicuro di usare un PC
 - Indipendentemente da firewall e antivirus

www.devleap.it

deVleap

Come fare il grande salto

- **Caratteristiche dell'utente:**
 - **No** gruppo Administrators
 - **No** gruppo Power Users
 - **Si** gruppo Users
- **Per uno sviluppatore**
 - **Creare un gruppo "Developer" o "Advanced User"**
 - Si definiranno le permission sul gruppo e non sull'utente
 - In caso di nuovi utenti sviluppatori sarà facile abilitarli
 - **Associare l'utente a tale gruppo**

www.devleap.it

deVleap

Come fare il grande salto

- **Tre strade:**
 - **Cambiare il proprio utente (amministratore locale della macchina) in un utente "normale"**
 - Problema: ciò che è già installato resta accessibile all'utente solo perché è owner di registry e directory
 - Si rischia di non percepire alcuni problemi
 - **Creare un nuovo utente**
 - Strada consigliabile
 - Si perdono i profili
 - **Reinstallare tutto**
 - Si perdono i profili
 - Si evitano "eredità" del passato
 - Ci vuole un sacco di tempo!!

www.devleap.it

deVleap

Prepararsi psicologicamente

- **Perché questo avvertimento?**
 - **Tanti programmi e tante operazioni non funzioneranno più come prima!**
- **I primi due giorni sono i più duri**
- **Ci saranno delle crisi...**
- **Resistete! Potete farcela!**
- **Dopo una settimana:**
 - Vi sentirete meglio di prima
 - Avvertirete un maggiore controllo sulla macchina
 - Vi chiederete come avete fatto prima

www.devleap.it

deVleap

RunAs

- **Il primo strumento da usare è RunAs**
- **Consente di avviare un programma con le credenziali di un altro utente**
 - Richiede un logon a ogni esecuzione
 - Si può fare uno script con le password in chiaro ma... bye bye security!
- **Va usato solo per le applicazioni che necessitano *realmente* di un amministratore:**
 - Configurazione di sistema
 - Console amministrative
 - FileMon, RegMon, ProcessExplorer

www.devleap.it

deVleap

Riparare le applicazioni scritte male

- **Individuare Registry e Directory di cui modificare le ACL**
 - Usare RegMon e FileMon
 - Di solito si trova un Access Denied poco prima dell'interruzione del programma
- **Abbassare al minimo indispensabile i diritti delle ACL**
 - Solo sulla directory interessata
 - Meglio (quando possibile) solo sul file interessato
 - Usare gruppo "Developer"/"Advanced User" piuttosto che il singolo utente

www.devleap.it

deVleap

Setup di Visual Studio .NET

- **Visual Studio .NET crea alcuni gruppi a cui uno sviluppatore deve appartenere:**
 - VS Developers
 - Debugger Users
- **Inserire a mano gli utenti sviluppatori in questi gruppi**
- **Alcune attività restano agli amministratori:**
 - **Registrazione di componenti COM (regsvr32/regasm)**
 - **Installazione di assembly nella GAC (gacutil)**
 - **Installazione di componenti .NET nel catalogo COM+ (regsvcs)**

www.devleap.it

deVleap

Problemi di debug

- **Gruppo Debugger Users**
 - **A questo gruppo è assegnato il privilegio SeDebugPrivilege**
 - Un virus potrebbe sfruttare questo privilegio per alcuni attacchi ai processi in esecuzione
 - Per le applicazioni .NET (managed) il debug al processo di un altro utente richiede utente admin
 - Non è così per applicazioni Unmanaged
- **Problemi per chi sviluppa servizi o siti web**
 - **Workaround: in debug eseguire il servizio/sito web con lo stesso utente con cui si fa il debug**
 - **Se debug remoto: richiesto privilegio SeDebugPrivilege anche su macchina remota**

www.devleap.it

deVleap

ASP.NET

- **Due modalità di connessione:**
 - **File Share**
 - È il default
 - Basta avere i diritti sul file system
 - **Front Page Server Extension**
 - Non si può creare una Virtual Directory da VS.NET
 - Articolo KB 833896
 - Creare la Virtual Directory manualmente
 - Usare un utente abilitato: VS Developers sul PC locale o un amministratore su un web server remoto
- Successivamente creare il progetto in VS.NET e connettersi alla Virtual Directory esistente

www.devleap.it

deVleap

Debug ASP.NET

- **Due aspetti**
 - **L'utente con cui gira l'applicazione**
 - Usare lo stesso utente con cui si sviluppa per fare debug
 - **I diritti sulle directory usate da ASP.NET**
 - Abilitare i diritti su tali directory all'utente con cui gira l'applicazione ASP.NET
- **Windows 2000/XP:**
 - L'utente associato a ASPNET_WP.EXE è uno solo per tutta la macchina
 - Workaround: eseguire VS.NET con RunAs_solo_ limitatamente alla fase di debug
- **Windows 2003:**
 - Gli application pool di IIS aiutano nella gestione di diverse applicazioni con credenziali differenti
- **Visual Studio 2005:**
 - Non esisteranno più questi problemi a prescindere da IIS, visto che in debug potremo usare "Visual Web Developer Web Server".

www.devleap.it

deVleap

Modifica utente ASP.NET

- **IIS 5 (fino a Windows XP)**
 - **Modificare tag processModel del file web.config**

```
<processModel enable="true"
  userName="DOMAIN\username"
  password="pwd" / >
```
 - Usare ASPNET_SETREG per cifrare la password senza lasciarla in chiaro (KB 329290)
- **IIS 6 (Windows 2003)**
 - **Creare un Application Pool**
 - **Assegnare utente sviluppatore all'application pool**
 - **Assegnare utente sviluppatore a gruppo IIS_WPG**
 - Altrimenti non funziona con ASP.NET
 - **Assegnare la Virtual Directory all'Application Pool**

www.devleap.it

deVleap

VB6

- **Brutte notizie**
- **Non è pensato per essere utilizzato da utenti non amministratori**
- **Si può ovviare con le tecniche descritte prima**
 - Usare FileMon e RegMon
 - Individuare punti in cui modificare le ACL
- **Molti problemi causati da componenti (ActiveX) di terze parti**
 - Anche qua si può ovviare con modifica di ACL
- **Problema: è un lavoro immane e si rischia di tornare al punto di partenza (bassa security)**

www.devleap.it

deVleap

Conclusione

- **La security è un problema di tutti, non solo di Microsoft**
- **Chiunque scriva software è parte del problema**
- **Ciascuno deve fare la sua parte**
- **Per cominciare:**
 - Scrivere applicazioni utilizzabili da utenti "normali"
 - Sviluppare con un utente non amministratore

www.devleap.it

deVleap

Link utili

- **Bug di Visual Studio, KB833896,**
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;833896>
- **Uso di aspnet_setreg, KB329290,**
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;329290>
- **Developing Software in Visual Studio .NET with Non-Administrative Privileges**
http://msdn.microsoft.com/library/en-us/dv_vstechart/html/tchDevelopingSoftwareInVisualStudioNETWithNon-AdministrativePrivileges.asp
- **Keith Brown - Libri e blog**
<http://pluralsight.com/blogs/keith/default.aspx>
- **Why non admin – Wiki**
<http://nonadmin.editme.com/WhyNonAdmin>

www.devleap.it

deVleap

Altre Informazioni

- **Dove posso ottenere maggiori informazioni**
 - www.devleap.com
 - blogs.devleap.com
 - msdn.microsoft.com
- **Developer resources**
 - Microsoft Visual Studio.NET
 - Microsoft .NET Framework SDK
 - Microsoft Developer Network



www.devleap.it

deVleap

Microsoft®

© 2002 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

www.devleap.it

deVleap