



Cybercrimes.it

Computer Forensics & Crimine Informatico

Dario Scalea

A DIFESA DEI BAMBINI

Strategie Telematiche Preventive ed Interposizionali

Realtà e Virtualità

Polimorfismo dell'apparire e monotonia dell'essere.

Il progresso tecnologico in ogni campo dell'agire umano ha sempre avuto come fine ultimo la riduzione dei tempi e degli spazi. Le reti di calcolatori sono l'asintote di questo concetto perchè consentono comunicazioni interattive multisensoriali con indice st infinitesimale progressivo. Questa caratteristica peculiare tesa alla massima convergenza possibile ha portato le reti di calcolatori a passare da strumento oligarchico per centri di ricerca con fini scientifici e/o militari a mezzo di comunicazione di massa talmente diffuso e pervasivo da evolversi e ramificarsi fino a diventare una traduzione integrale del mondo fisico così come ci è maggiormente noto. Le problematiche etiche derivanti sono tutte contenute propriamente in quell'aggettivo: integrale. Davanti ai dispositivi di input di ogni calcolatore siede un essere umano che compie una serie di scelte binarie secondo la propria natura e formazione. Purtroppo o per fortuna (a seconda dei casi), natura e formazione sono costanti indipendenti dalla dimensione operativa. Nel bene e nel male l'essere umano reale e l'essere umano virtuale sono identici. L'obbiettivo di questo testo è fornire gli strumenti per comprendere come migliorare la difesa del bambino dai pericoli che questa identità comporta. In quasi tutte le famiglie esiste almeno una persona che ha conoscenze utente dei pc: a voi è rivolto il mio testo e alla vostra sensibilità mi appello nel pregarvi di applicare queste semplici contromisure per tutelare i vostri parenti bambini. Trattandosi di materiale destinato alla pubblicazione e quindi inevitabilmente ad un insieme indiscriminato di lettori, mi scuserete se, per motivi etici, ometterò spiegazioni low-level e mi limiterò ad un grado di specificità che non consenta l'utilizzo reversibile delle informazioni.

Tassonomia dimensionale e sicurezza infantile.

Conoscere la struttura dello scenario applicativo è un elemento cruciale nella pianificazione di ogni genere di strategia. A partire dalla dimensione reale induciamo 4 fattori essenziali di differenziabilità:

- 1) Materialità**
- 2) Fisionomia**
- 3) Intervallabilità**
- 4) Orientabilità**

Segnatamente la dimensione virtuale postula la loro negazione in quanto:

- 1) Non esiste impedimento fisico.**
- 2) Non esiste riconoscimento fisionomico incondizionato.**
- 3) Non esiste intervallo spaziale tra due punti.**
- 4) Non esiste orientamento tra risorse senza specifiche conoscenze.**

Poiché la sicurezza dell'utente bambino è inversamente proporzionale alla relazionabilità con altri utenti o contenuti e la relazionabilità dipende dalle suddette proprietà possiamo legittimamente inferire che :

$$S_b = R^{-1}$$

$$R = \frac{(A \cdot B \cdot C \cdot D_u \cdot D_b)}{N}$$

$$\left\{ \begin{array}{l} A = \max \\ B = 1 \\ C = \max \end{array} \right.$$

Da notare che R è uguale al rapporto tra un prodotto (di tre costanti e due variabili) e una variabile. Le tre costanti sono:

il valore di accessibilità collettiva A

(massimo in quanto non esistono impedimenti fisici);

il valore di riconoscibilità fisionomica B

(uguale a 1 perchè elemento neutro del prodotto in quanto l'anonimato fisionomico dell'utente bambino ostacola la relazionabilità ma l'anonimato fisionomico dell'utente altro la favorisce);

il valore di vicinanza collettiva C

(massimo perchè non esiste intervallabilità);

Le due variabili sono:

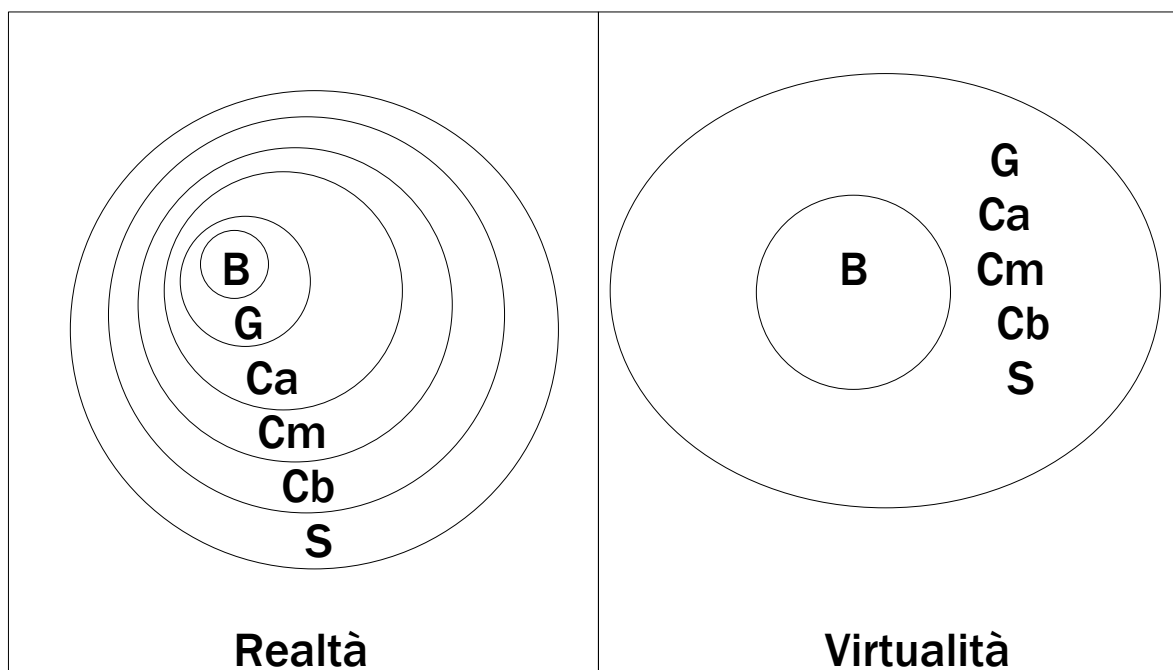
il valore di capacità dell'utente altro D_u e dell'utente bambino D_b

(basta che uno dei due sia uguale a zero ovvero uno dei due non sappia usare il calcolatore per rendere impossibile la relazionabilità. Purtroppo, a differenza del valore B, anche la capacità del bambino favorisce la relazionabilità in quanto lo stadio dello sviluppo cognitivo che gli è proprio non consente di percepire minacce complesse).

il valore di numerosità N

(maggiore è il numero di utenti più difficile diventa la relazionabilità specifica).

Da questa formula si desume facilmente che, in fase di approccio, il campo virtuale è molto più pericoloso di quello reale. Questo appare evidente anche nella rappresentazione grafica dei soggetti di relazione:



Simbolo	Soggetto di relazione
B	Bambino
G	Genitore
Ca	Conoscente ad alta frequentazione
Cm	Conoscente a media frequentazione
Cb	Conoscente a bassa frequentazione
S	Sconosciuto

Topologia della relazionabilità infantile e rischi relativi.

La relazionabilità infantile agisce in funzione di due categorie complementari definite dagli estremi della comunicazione: a) interazione bambino-macchina, b) interazione bambino-umano. Ognuna di queste categoria corrisponde a un rischio relativo esprimibile a sua volta in funzione di due variabili: movente e tipo. Ovviamente la r.i. è compresa nell'intervallo temporale d'inizio e fine sessione comunicativa.

Analiticamente:

$$\Omega = \int_{\tau_0}^{\tau_1} f\{x[\xi_1(h,k)], y[\xi_2(h,k)]\} dx dy$$

RELAZIONABILITÀ			
Interazione A		Interazione B	
Rischio relativo			
Tipo	Movente	Tipo	Movente
Visualizzazione CIFSC*	Economico Politico Apologetico Divulgativo Persuasivo	Adescamento	Pedofilia
Sottrazione danneggiamento dati	Estremamente diversificati	Circonvenzione	Social Engineering

*(Contenuti impropri alla fase dello sviluppo cognitivo)

Etologia infantile

Sviluppo cognitivo

I rischi relativi alla navigazione in Internet sono in larga misura dipendenti dal modo di operare dall'utente. L'etologia ha un suo importante generatore nello sviluppo cognitivo. In questo campo i passi che restano da fare sono molti di più di quelli fatti dal momento che i contributi delle neuroscienze alla spiegazione della meccanica, della dinamica e dell'evoluzione cerebrale sono lenti e tanti restano gli interrogativi a cui manca una risposta. A colmare queste lacune ci provano alcuni rami della psicologia che, è bene ricordarlo, non è una forma di conoscenza nata dal metodo scientifico-sperimentale e quindi non può essere considerata una scienza (anche se pare che oggi questo termine non si neghi a nessuno). Quindi ci dobbiamo necessariamente affidare alla disciplina dei discorsi sull'anima, ma vi esorto a prendere le nozioni che seguiranno per quello che sono: opinioni. I migliori studi sullo sviluppo cognitivo infantile sono stati fatti dal biologo Jean Piaget che si propose lo scopo di creare una teoria della formazione della conoscenza, definita epistemologia genetica. Per questo fondò a Ginevra il Centro studi di epistemologia genetica avvalendosi della determinante collaborazione di matematici e fisici. La teoria di Piaget, nel periodo evolutivo che va dai 4 ai 14 anni, traccia il seguente sviluppo:

a) Pensiero intuitivo

$$\{a_1 \wedge a_2 = a\} \in \perp$$

b) Identità qualitativa e concetto di funzione

$$\{a_1 \wedge a_2 = a\} \notin \perp \quad y = f(x)$$

c) Pensiero reversibile

$$\forall x \in U \exists y: y = 1/x$$

d) Classificazione per estensione e definizione in collezioni figurali e non figurali

$$(x \in P \Rightarrow x \subseteq X)(y \in D \Rightarrow y \subseteq Y) \quad \forall (x \vee y) \in \{[C = (\sum_{k=a}^z h_k)] \oplus (Ps \neq C)\}$$

e) Moltiplicazione logica fra classi

$$X \cap Y = \{x \in P: x \in X \text{ e } x \in Y\}$$

f) Operazioni di seriazione

$$s_n = \lim_{n \rightarrow \infty} \sum_{k=1}^n a_k \quad n=p$$

g) Seriazione moltiplicativa

$$s_{x,y} = \left(\lim_{x \rightarrow \infty} \sum_{k=1}^x a_k \right) \left(\lim_{y \rightarrow \infty} \sum_{h=1}^y a_h \right)$$

h) Operazioni di numerazione come sintesi per classe e per serie

$$a_{(x,y)} \sim b_{(v,z)} \quad \forall a_{(x,y)} \in Z_1, b_{(v,z)} \in Z_2$$

i) Operazioni infralogiche

$$\{\sim\} \in X_{(s,t) \vee (p/h,h)}$$

l) Gruppo INRC

$$\text{INRC} = A_{\{-\}} = \{x, -x, 1/x, -1/x\}$$

m) Logica delle proposizioni

$$L_p = \{A, B, \dots, Z\} \cup \{\neg, \wedge, \vee, \Rightarrow, \perp\} \cup \{“”, “”\}$$

Questo sistema evolutivo ha il merito di essere più rigoroso e coerente di altri ma non per questo è stato esente da critiche e revisioni. Trattandosi di una sommatoria progressiva capirete che meno proprietà cognitive possiede l'utente (tendenti al limite dell'alfabetizzazione informatica) più è esposto ai rischi. L'ordinamento rende possibile approntare strategie difensive diversificate.

Un modello virtuale: la rete di calcolatori

A questo punto possiamo procedere ad analizzare il modello virtuale per antonomasia: la rete di calcolatori.

Storia

La nascita della rete è dovuta all'esigenza di comunicazione tra calcolatori. Nel 1961 Kleinrock pubblicò uno studio sulla commutazione di pacchetto (packet switching). Nel 1969 la BBN (Bolt Beranek and Newman) vinse il concorso bandito dall'ARPA (Advanced Research Projects Agency) e nacque ARPANET. Arpanet comunicava tramite il protocollo NCP ed era costituita inizialmente da quattro computer host: UCLA a Los Angeles, UC di Santa Barbara, università dello Utah e Stanford Research Institute. Nel 1974 Cerf e Kahn inventarono il protocollo TCP/IP (Transmission Control Protocol/Internet Protocol) che sostituì NCP ed è ancora oggi lo standard di riferimento. Intorno agli anni novanta Arpanet fu sostituita da NSFNet. Nel 1992 il CERN introdusse il concetto di WWW (World Wide Web) e nel 1994 nasce il protocollo PPP (Point to point Protocol). Da qui in avanti la rete conosce una crescita esponenziale fino a conquistare il primato comunicativo mondiale.

Anatomia

Per capire come e dove intervenire oltre all'analisi dimensionale dobbiamo conoscere la specifica architettura interna allo scenario applicativo. Questa è regolata in base al modello di riferimento OSI (Open Systems Interconnection) sviluppato dall'ISO (International Organization for Standardization) nel 1979. Il modello OSI divide una sessione di comunicazione in sette livelli funzionali:

① Physical

Livello che gestisce il bitstream esclusivamente in base ai parametri fisici della trasmissione.

② Data Link

Livello responsabile del partizionamento in frame del bitstream e dell'integrità dei dati sull'asse ricezione-trasmissione con verifica ed eventuali correzioni.

③ Network

Livello che ha il compito di indirizzare i frame all'esterno della LAN tramite routed protocols.

④ Trasport

Livello responsabile dell'integrità extraLAN dei dati e del riposizionamento sequenziale dei pacchetti.

⑤ Session

Livello che gestisce il datastream tra due sistemi (direzionalità, token, synchronization).

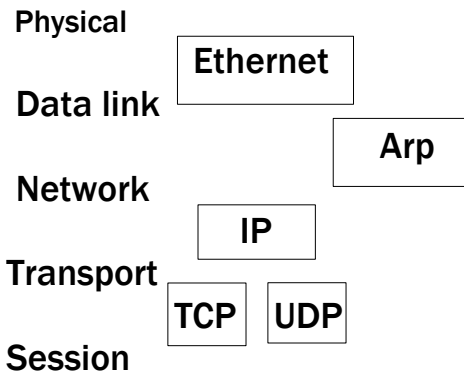
⑥ Presentation

Livello responsabile della codifica dati.

⑦ Application

Livello che interfaccia le applicazioni utente con i servizi di rete.

Ora possiamo procedere alla mappatura del nostro ambiente operativo:



Presentation

Application(essential)

PROTOCOL	http	msnp	Edonkeyext.	irc	smtp	pop3	netbios	https	ftp	nntp	telnet	whois	finger
PORT	80	1863	4662	194	25	110	139	443	21	119	23	43	79

PROTOCOL	dns	kerberos	imap	mi.di.se.	wins	pptp	
PORT	53	110	143	445	1512	1723	

In una rete di calcolatori si può comunicare con l'esterno attraverso quelle che in gergo vengono definite porte. Ogni porta è identificata da un numero binario a 16 bit, pertanto sono matematicamente possibili 65.535 porte. La totalità delle porte è stata divisa in tre categorie: note (0-1023), registrate (1024-49151), dinamiche o private (49152-65535). Poiché le possibili minacce per il bambino vengono dalla comunicazione con l'esterno, ci appare evidente l'importanza di operare un controllo su queste porte. Ma un'unica contromisura potrebbe non essere sufficiente. Così, dall'esigenza di un intervento integrato, ho sviluppato l'OSI Child protection model.

OSI Child Protection model

A partire dal modello OSI ho elaborato una strategia multilivello che ha l'obiettivo di controllare le attività e ridurre il potenziale comunicativo del calcolatore all'esigenze operative del bambino proporzionandolo alla fase dello sviluppo cognitivo per minimizzare il fattore di rischio relativo.

LIVELLO	CONTROMISURA	TIPOLOGIA
Physical	Keylogger hardware, network tap	Controllo interposizionale filtro preventivo
Data link	Arp configuration	Controllo interposizionale
Network	walled garden(ip filter)	Filtro preventivo
Trasport	P.filter,kernel pf,h.stack	Filtro preventivo
Session	H.duplex,synch points	Controllo interposizionale
Presentation	Cryptography	Controllo interposizionale
Application	Port Blocking	Filtro preventivo
Execution	Os conf and elision	Controllo interposizionale,elisione e filtro preventivo

Per le motivazioni già esposte all'inizio sono presenti solo alcune contromisure e tra queste di seguito presenterò i tratti essenziali delle principali.

Keylogger hardware

Questo dispositivo vi consente di sapere cosa viene digitato sulla tastiera.

Il keylogger hardware è una contromisura di livello fisico. Le contromisure di questo livello sono le più sicure perchè non consentono una elusione da remoto. Come principio più basso è il livello a cui si interviene, più alto è il margine di sicurezza. Il keylogger è uno strumento di intercettazione e memorizzazione dell'input proveniente da tastiera. Può essere applicato in diversi punti ma tre sono quelli che hanno riscosso l'interesse del mercato: tra i connettori (cavo-pc), interno alla tastiera, interno al pc. Potete scegliere la soluzione che volete ma ricordate:

- 1) Nel caso preferite utilizzare il keylogger tra i connettori fate in modo che non possa essere staccato.
- 2) Non controllate mai il contenuto del keylogger dallo stesso pc su cui viene installato.
- 3) Se scegliete la prima o la seconda soluzione, assicuratevi che non ci siano altre tastiere a portata di mano.
- 4) Procedete all'unlinking della tastiera virtuale (contromisura di livello

esecutivo,ma mi sembra corretto inserirla qui) dalla shell dei comandi a 32 bit (cmd.exe) digitando:

del %path:~0,19%\osk.exe

(Il sistema operativo preso in considerazione è Windows Xp SP2 Professional,perchè i sistemi gui dos-native per semplicità e diffusione sono i più utilizzati dai minori)

Walled garden

Il walled garden(giardino murato)è un tipo di protezione che restringe lo spazio comunicativo consentendo la connessione soltanto a dei numeri predefiniti di protocollo internet.Utilizzare un filtro negativo(vietare tutto tranne le eccezioni) è senza dubbio la soluzione che offre le migliori garanzie ma è anche la più limitante.Il filtro può essere applicato in diversi modi e in diversi punti(router firmware,kernel,proxy server, firewall hs-ware,browser).Un equilibrato compromesso tra semplicità ed efficacia si può trovare con l'ibrido seguente:Eseguite Internet Explorer.Digitate Alt,s,o.Selezionate la scheda Contenuto ,poi Attiva.Assicuratevi che nella scheda Classificazioni sia impostato il livello 0.Selezionate la scheda Siti approvati,inserite nel campo sottostante il nome del sito consentito e selezionate Sempre.Ripetere le ultime due operazioni un numero di volte pari al numero totale dei siti consentiti che volete inserire.Portatevi alla scheda Generale e accertatevi che le Opzioni utente NON siano selezionate,create la password del supervisore e applicate.Aggiungete il valore dword ContentTab , modificando il valore dati in 1, alla chiave HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer \Control Panel.Ricordate di configurare il windows firewall in modo che Internet Explorer sia l'unico browser utilizzabile e vengano negate tutte le porte eccetto quelle necessarie alla navigazione.

Xp consente altri metodi di restrizioni ip intermedi come Criterio di gruppo(start-esegui-gpedit.msc) ,file hosts,netsh da riga di comando.Se desiderate soluzioni più avanzate potete iniziare utilizzando Winpcap che filtra i pacchetti a livello kernel fino ad arrivare a interrogazioni a risoluzione inversa mediante puntatori sui record A (DNS) o per riferimenti diretti normalizzati a 32 bit sulla testata ip(Hip≥20 ottetti)nei campi source/destination address.

Os configuration

Tra la miriade di risultati difensivi ottenibili agendo sul sistema operativo vediamo come ottenere la registrazione dell' attività di web browsing.Con questa finalità ho scritto un elementare batch file.

Aprirete il blocco note e scrivete quanto segue:

```

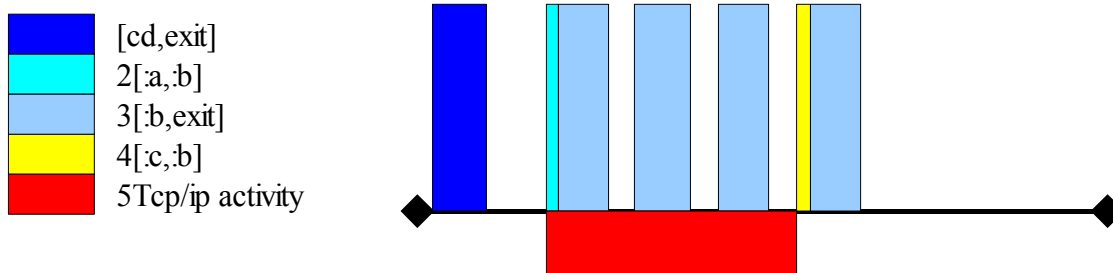
@echo off
cd %Path:~0,19%
%1
cscript //h:cscript //s
eventtriggers /create /tr inizio /l system /eid 4201 /tk "%~fs0 goto:a" /ru %username% /rp inserirepassword
eventtriggers /create /tr fine /l system /eid 4202 /tk "%~fs0 goto:c" /ru %username% /rp inserirepassword
reg add "hkcu\Software\Policies\Microsoft\Windows\Task Scheduler5.0" /v "Task Deletion" /t reg_dword /d 1 /f
reg add "hkcu\Software\Policies\Microsoft\Windows\Task Scheduler5.0" /v Execution /t reg_dword /d 1 /f
reg add "hkcu\Software\Policies\Microsoft\Windows\Task Scheduler5.0" /v "Property Pages" /t reg_dword /d 1 /f
reg add "hkml\Software\Policies\Microsoft\Internet Explorer\Control Panel " /v GeneralTab /t reg_dword /d 1 /f
for /d %%x in (content.dll history.dll cookie.dll analisi.dll) do ver>>%%~x && attrib +s +h %%~x
attrib +s +h %~fs0
exit
:a
schtasks /create /tn ciclo /tr "%~fs0 goto:b" /sc minute /mo 5 /ru %username% /rp inserirepassword
:b
for /d %%x in (content.dll history.dll cookie.dll) do (date/t&time/t) >>%%~x
type %tmp%or~1\Content.IE5\index.dat >>content.dll
type %tmp:~0,-4%CRONOL~1\History.IE5\index.dat >>history.dll
type %tmp:~0,-13%Cookies\index.dat >>cookie.dll
(date/t & time/t & tasklist/svc & netstat -er & netstat -abnov) >>analisi.dll
exit
:c
schtasks /delete -tn ciclo /f && %~fs0 goto:b

```

Sostituite Inserirepassword con la password dell'account utente,selezionate salvate con nome e scrivete nome.bat.Eseguite il file(per vedere i comandi eliminate la stringa @echo off,per non visualizzare la finestra incapsulare il batch in un vbscript con una chiamata ad oggetto Wshshell.Run()). All'inizio dell'attività di rete, il calcolatore pianificherà una serie di istruzioni cicliche che ogni cinque minuti impilerà l'output dei files index.dat nei file content.dll,cookie.dll e history.dll contenuti nella directory C:\windows\system32\ e monitorerà i processi in esecuzione con relativi servizi, dll e porte associate più la tabella di Route e statistiche generali reindirizzando l'output nel file analisi.dll.Alla fine dell'attività di rete,verrà cancellata la pianificazione ed eseguita la serie un'ultima volta.Ricordate che, alla prima esecuzione del file senza passaggio di argomenti, verrà impedita la cancellazione,l'esecuzione,la terminazione e la visualizzazione delle proprietà manuale da gui delle operazioni pianificate e verrà tolta la scheda generale del browser.Inoltre se non utilizzate un router ma un modem dsl per la connessione sostituite gli id 4201(scheda di rete connessa e inizio delle operazione,libreria a collegamento dinamico netevent.dll) e 4202(scheda di rete disconnessa,netevent.dll.In alternativa id 8033 impostazione d'elezione sulla rete con arresto del master,netevent.dll) con gli id 20158(l'utente ha stabilito la connessione,mprmsg.dll-iassvcs.dll) e 20159(la connessione è stata interrotta,mprmsg.dll-iassvcs.dll):questo algoritmo delimita l'intervallo esecutivo

con gli event logs del sistema operativo, per evitare coincidenze potete aggiungere il parametro /so Tcpip per gli eventi 4201-4202 e il parametro /so RemoteAccess per gli eventi 20158-20159. Verificate la presenza degli id precedenti nel registro system con il comando eventquery /l system, se non ci sono createli. Ovviamente si tratta solo di un esempio ampiamente implementabile.

timeline nome.bat



Per visualizzare i risultati in modo sintentico potete filtrare i files con i seguenti comandi:

```
cd %comspec:~0,19%
find /i "http" content.dll >>content.txt
find /i "visited" history.dll >>history.txt
find /i "cookie" cookie.dll >>cookie.txt
```

Vi basterà aprire i suddetti file di testo per vedere i siti visitati, ma vi consiglio di consultare anche le dll per maggiori informazioni. Inoltre cancellate i file dopo la consultazioni perchè altrimenti diventano di dimensioni eccessive e quindi difficilmente gestibili. Per cambiare la frequenza di memorizzazione vi basterà modificare il parametro /mo al comando schtasks digitando come valore il numero di minuti desiderato.

Tramite l'editor del registro di sistema possiamo rendere meno facili (considerata la tipologia di utente) modifiche ai parametri del sistema operativo da cui dipende il funzionamento di x.bat e la sicurezza della connessione. Dalla shell dei comandi (o più semplicemente con regedit):

```
reg add hklm\Software\Microsoft\Windows\CurrentVersion\Policies\explorer /v nocontrolpanel /t reg_dword /d 1 /f
reg add hklm\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile /v EnableFirewall /t reg_dword /d 1 /f
reg add hklm\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile /v DisableNotifications /t reg_dword /d 1 /f
reg add hkcu\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t reg_dword /d 1 /f
reg add hkcu\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\explorer /v StartMenuLogOff /t reg_dword /d 1 /f
reg add hkcu\Software\Policies\Microsoft\MMC /v RestrictToPermittedSnapins /t reg_dword /d 1 /f
```

```
reg add hkcu\Software\Policies\Microsoft\Messenger\Client /v PreventRun /t reg_dword /d 1 /f
```

```
reg add hkcu\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableRegistryTools /t reg_dword /d 1 /f
```

(Per rimuovere Messenger andate in Start-Run e digitate:

```
RunDll32 advpack.dll,LaunchINFSection %windir%\INF\msmsgs.inf,BLC.Remove)
```

Parental control software

Uno, nessuno o centomila?

Il parental control software è un programma progettato per svolgere la funzione di controllo genitoriale del sistema su cui è installato. L'ambizioso e lodevole proponimento ha diffuso l'erronea convinzione che l'utilizzo di un software di questa tipologia sia sufficiente a garantire la totale protezione dell'attività informatica del bambino. Per questo è bene precisare quanto segue:

1) La sola esecuzione di un parental control software (anche se dotato di "stealth" mode o residente su server) è in sé molto pericolosa perché fornisce la possibilità di sapere da remoto, con ragionevole certezza deduttiva, se il computer viene utilizzato da un bambino.

2) Nessun crawler è in grado di garantire la classificazione di tutti i contenuti internet. Quindi nessun software può avere un filtro web efficace al 100%.

3) Attivare un filtro chat per impedire la divulgazione di informazioni sensibili significa fornire la possibilità permanente di accedere da remoto a queste informazioni (precisamente alle loro hashes) perché il filtro lavora con una procedura di esclusione per confronto.

4) Come in ogni software, esistono una serie di vulnerabilità del codice.

Fortunatamente per rendere effettivi la maggior parte dei pericoli è richiesta una competenza tecnica medio-alta o applicazioni specifiche equivalenti. Questo rende il fattore di rischio marginale ma non trascurabile (in alcuni casi, vedi punto 1, addirittura discriminante). In definitiva, i p.c.s. posso avere un rapporto di utilità rischi/benefici positivo ma non garantiscono una protezione completa.

L'importanza del dialogo

Tra tutte le contromisure di tutela che si possono adottare, sia nel campo della virtualità che della realtà, ce n'è una fondamentale ed insostituibile: il dialogo tra il bambino e i genitori. Qualsiasi strategia di adescamento si basa sulla fiducia e sull'omertà. Dite ai vostri bambini che tutti i motivi che verranno adottati da chi cerca di persuaderli a non parlare con mamma e papà sono falsi, che parlare con mamma e papà non causerà mai qualcosa di brutto a lui e alle persone che vuole bene. Ricordate che le informazioni più importanti per la tutela del bambino vengono proprio dal bambino stesso.

Dario Scalea