Milano, 13 giugno 2007

Spett.le
Ministero dell'Interno
Dipartimento della pubblica sicurezza –
Direzione centrale per la Polizia Stradale, Ferroviaria, delle comunicazioni e per i reparti speciali della Polizia di Stato.
Piazzale Del Viminale, 1
00184 Roma (RM)

Offerta n. 20070319.10v5.0GP

Oggetto: Offerta fornitura software "RCS"

A seguito dei colloqui intercorsi vi sottoponiamo la nostra migliore proposta per il software in oggetto.

In attesa di un vostro gradito riscontro, vi porgiamo i nostri più cordiali saluti.

Hacking Team Srl

Gabriele Parravicini
Responsabile commerciale

Offerta
Fornitura software “RCS”

SOMMARIO

1. STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	28 marzo 2007	Emissione
2.0	29 marzo 2007	Modifica
3.0	24 maggio 2007	Modifica
4.0	28 maggio 2007	Modifica
5.0	13 giugno 2007	Modifica

2. RICHIESTA DEL CLIENTE

Il Servizio di Polizia Postale e delle comunicazioni richiede di formulare una proposta con relativa offerta economica, per la fornitura, basata sulla specifica esigenza non pubblicabile del Servizio stesso, del software denominato “RCS”, della relativa manutenzione e degli apparati hardware necessari al suo corretto funzionamento.

In altre parole, si richiede un’offerta di: licenza d’uso del software “RCS” della relativa manutenzione e dell’hardware necessario.

3. SOLUZIONE PROPOSTA

La fornitura proposta si compone delle seguenti parti:

- 1 Licenza sofware “RCS” illimitata nel tempo
- 1 Licenza modulo aggiuntivo VoIP - Skype
- 1 licenza modulo Hacking resources
- 2 server adeguatamente dimensionati e configurati
- manutenzione per 24 mesi su tutti i moduli

4. DESCRIZIONE PRODOTTO

Nel presente capitolo vengono introdotti i concetti chiave del prodotto Remote Control System, sviluppato da Hacking Team Srl.

4.1. Sicurezza offensiva

RCS è uno strumento per investigazioni invisibile pensato per gli organi di polizia, per le istituzioni e le agenzie governative. Permette il monitoraggio passivo e il controllo attivo di tutti i dati e i processi presenti sul PC remoto sotto indagine. I PC sotto indagine posso essere connessi ad Internet oppure totalmente isolati.

4.2. Funzionalità

RCS permette l’ intercettazione, il monitoraggio e la cattura di una moltitudine di attività sul computer remoto sotto indagine.

Ad esempio sono possibili le seguenti attività di intercettazione:

- Siti web visitati
- Documenti create/editati/salvati sul PC

- Qualsiasi tipo di tasto premuto, comprese password, nomi, chiavi di accesso
- Qualsiasi documento stampato dal PC
- Qualsiasi tipo di comunicazione voce per mezzo di VoIP - Skype
- Esecuzione di task remoti
- Upload/Download di qualsiasi file presente sul PC
- Snapshot dello schermo

4.3. Invisibilità

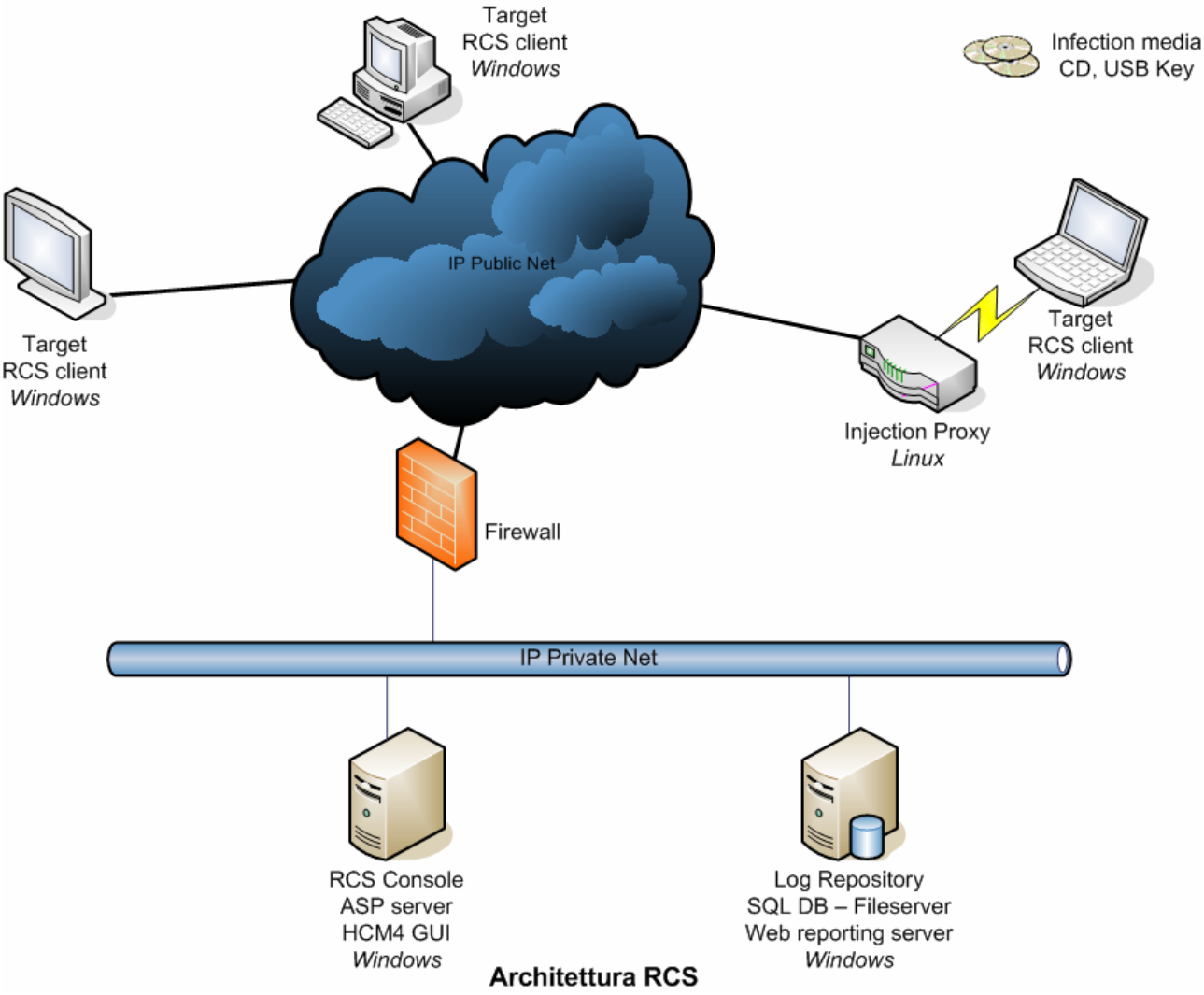
La caratteristica più valevole di RCS è l' invisibilità. Forte di una tecnologia proprietaria allo stato dell' arte, la componente client di RCS è in grado di mimetizzare la propria presenza sul computer oggetto dell' indagine in modo estremamente efficace.

L' utente sotto monitoraggio, pur essendo esperto e dotato di strumenti di protezione non avrà la capacità di rilevare alcuna anomalia sul proprio PC.

RCS risulta invisibile e resistente alla maggior parte dei sistemi di protezione personale oggi disponibili sul mercato, come ad esempio antivirus, anti-spyware, personal firewalls, network monitors, process monitors, anti-keylogging systems.

Il team di sviluppo di Hacking Team è attivamente impegnato sull' analisi e lo studio dei nuovi sistemi di protezione, in modo tale da poter sviluppare aggiornamenti allo strumento che garantiscano l' efficacia dello strumento nel tempo.

4.4. Architettura di riferimento



Architettura RCS

4.5. Target – RCS Client

Le caratteristiche di monitoraggio e intercettazione del prodotto avvengono per mezzo di una componente client molto piccola e leggera in termini di dimensioni e requisiti computazionali.

Il design del modulo client è modulare, nuove funzionalità di intercettazione posso essere installate da remoto senza dover ricorrere a operazioni manuali complicate e senza la necessità di effettuare il reboot della macchina sotto indagine.

La configurazione del modulo avviene automaticamente da remoto in modo trasparente.

La logica di funzionamento del modulo client di RCS si basa sul meccanismo Eventi->Azioni, in altre parole, ad ogni evento monitorato (es. traffico di rete, ora/data, programma in esecuzione,..) è

possibile associare una specifica azione (es. sincronizzazione con la Console, disinstallazione, riconfigurazione del modulo,..). Le combinazioni possibili sono illimitate.

Il modulo RCS Client, una volta installato e configurato, è in grado di funzionare autonomamente, senza la necessità di avere una connessione permanente con la stazione di controllo.

Le informazioni raccolte durante l' attività investigativa sono archiviate e cifrate localmente, e successivamente trasferite alla stazione di raccolta dei log con cadenza periodica e configurabile.

4.6. RCS Console

E' la stazione di controllo principale del prodotto RCS.

L' applicazione grafica HCM4 permette la gestione della maggior parte delle attività inerenti lo strumento, come ad esempio creazione di nuovi moduli client, configurazione, reportistica web, playback comunicazioni Skype.

Il modulo interno ASP è responsabile della sincronizzazione tra i computer sotto indagine e la stazione di controllo.

In altre parole il modulo ASP è costantemente in ascolto sulla rete in attesa di connessioni da parte dei moduli RCS client. Il filtraggio delle connessioni deve essere garantito da un firewall perimetrale con policy opportune.

ASP è dotato di un meccanismo di protezione aggiuntivo che in presenza di connessioni originate da normali browser è in grado di restituire una pagina web customizzabile, in modo tale da occultarne la presenza sulla rete (es. pagina di google o web stats).

4.7. Log repository

E' il server dove vengono archiviate le configurazioni di tutte le istanze di RCS Client e tutti i dati raccolti durante le attività investigative.

Dal punto di vista logico si compone di tre elementi: un database SQL, responsabile della struttura indice dei dati, un web server Apache, responsabile delle funzionalità di reporting, un fileserver Netbios, dove logicamente sono archiviati i file di configurazioni e le evidenze delle attività investigative. L'applicazione HCM4 GUI accede automaticamente al fileserver e al database SQL durante le normali operazioni di amministrazione e configurazione dello strumento. Sono previste credenziali di accesso con differenti livelli di autorizzazione.

4.8. Infection media

La prima installazione del modulo client di RCS risulta altamente critica per il successivo funzionamento del prodotto.

Le tecniche di intrusione remota sono molteplici e cambiano in relazione allo scenario operativo, a supporto dell' installazione di RCS sono disponibili una serie di vettori di infezione con differenti livelli di criticità e conseguenti capacità di successo.

Il prodotto RCS include una serie di meccanismi di infezione sia remota che locale:

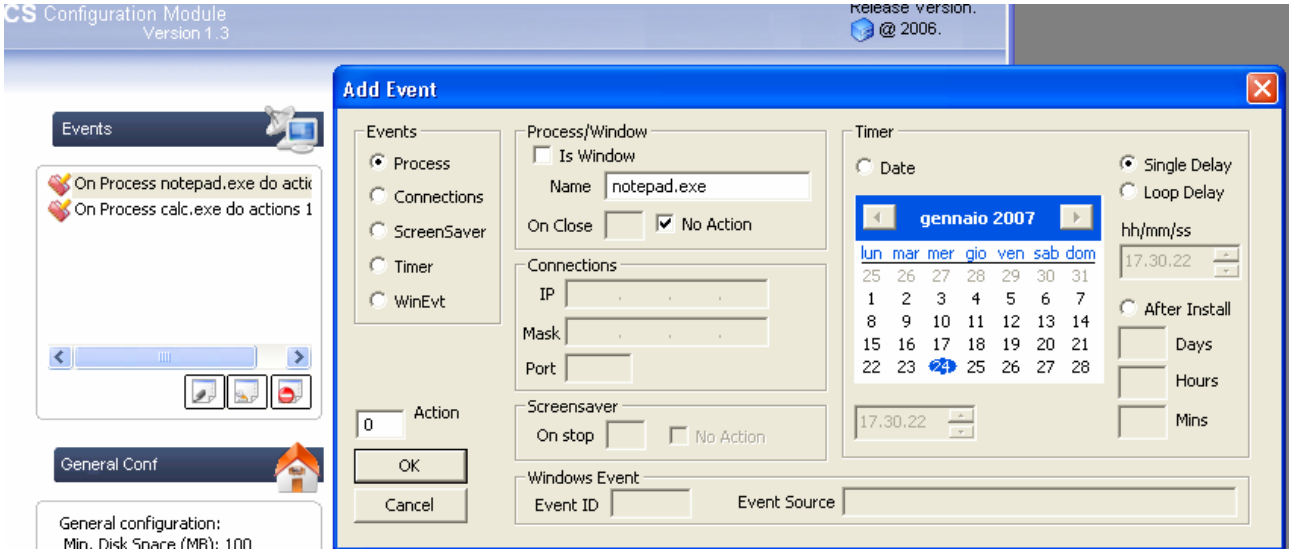
- Eseguibile windows (polimorfico, anti reversing, cifrato)
- Strumento di fusione eseguibili (payload cifrato e polimorfico)
- CD di installazione online e offline
- Injection Proxy

4.9. Caratteristiche

La configurazione del modulo client di RCS avviene mediante l' interfaccia grafica di amministrazione HCM4. Vengono elencate le caratteristiche principali del prodotto.

4.10. Configurazione eventi

Attraverso la finestra eventi di HCM4 è possibile configurare il monitoraggio degli eventi del sistema RCS a cui vengono successivamente associate una o più azioni corrispondenti.



Il modulo client di RCS è in grado di riconoscere i seguenti eventi:

- Esecuzioni/terminazione programmi o nomi finestre (es.notepad.exe, *mail*)
- Connessioni tcp indirizzo/netmask/porta/wildcards (es. *.80)
- Attivazione/disattivazione screensaver (es. screen locked)
- Timer di tipo ora/data
- Timer di tipo ciclico (ogni x sec.min.ore)
- Eventi di tipo windows

4.11. Configurazione azioni

La configurazione delle azioni associate a determinati eventi, avviene mediante uno specifico controllo presente in HCM4.

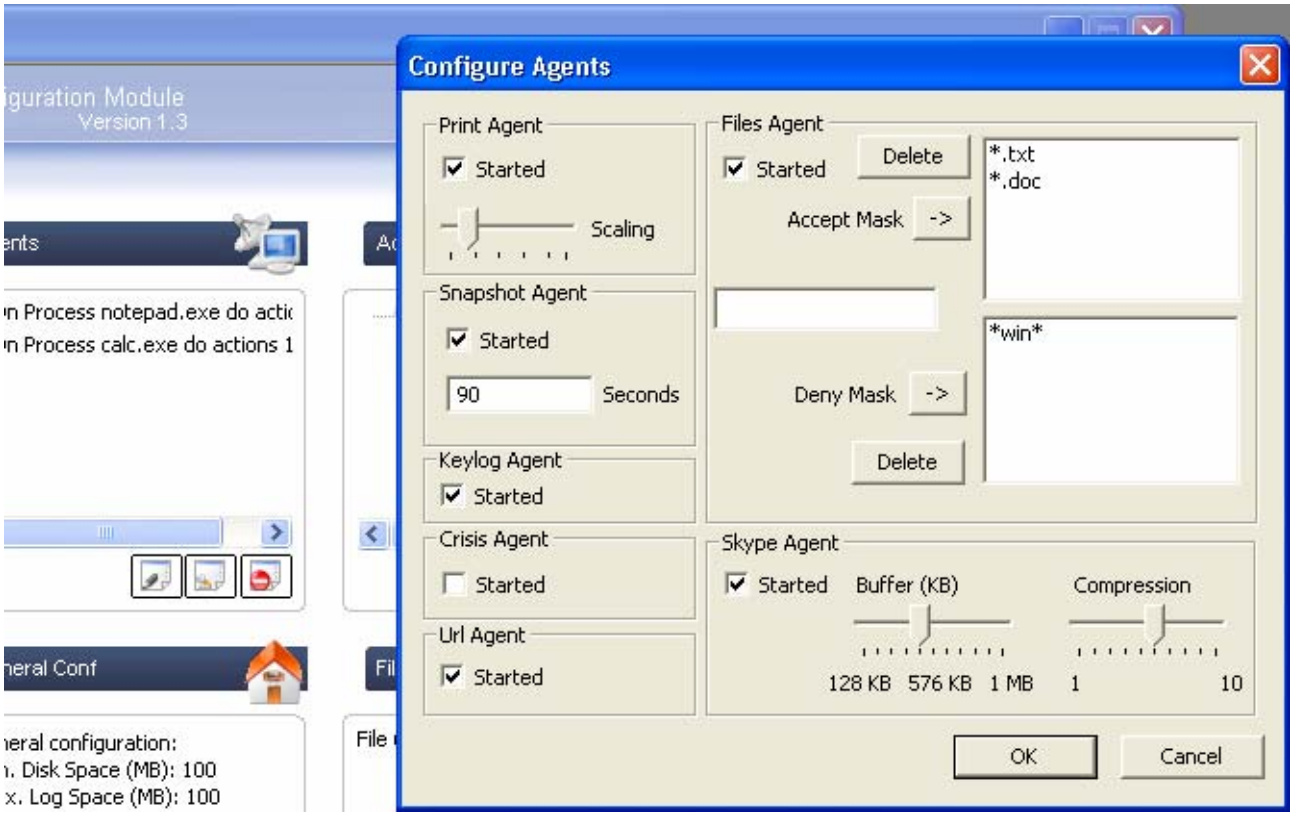
Il modulo client è in grado di associare le seguenti azioni:

- Syncronize
  - Attraverso la sync il modulo client invia tutte le evidenze di indagine alla console e contestualmente è in grado di accettare nuove configurazioni o moduli
  - E' supportata una limitazione di banda
- Agent start/stop
  - E' possibile attivare o disattivare il funzionamento di uno specifico agente di intercettazione (es. keylog stop, skype start).

- Uninstall
  - E' possibile rimuovere totalmente la presenza del modulo client, ivi compresi i log, le configurazioni, le chiavi dei registri, i processi in memoria.E' supportato il wiping.
- Command
  - Essendo la comunicazione asincrona è impossibile ottenere un controllo remoto di terminale tipo shell, è tuttavia supportata l' esecuzione remota di programmi o comandi. L' esecuzione avviene in modalità nascosta.

4.12. Agenti di intercettazione

L' attività di intercettazione avviene mediante agenti specifici, la cui configurazione avviene mediante apposito pannello di controllo presente in HCM4.



Gli agenti di intercettazione attualmente disponibili sono:

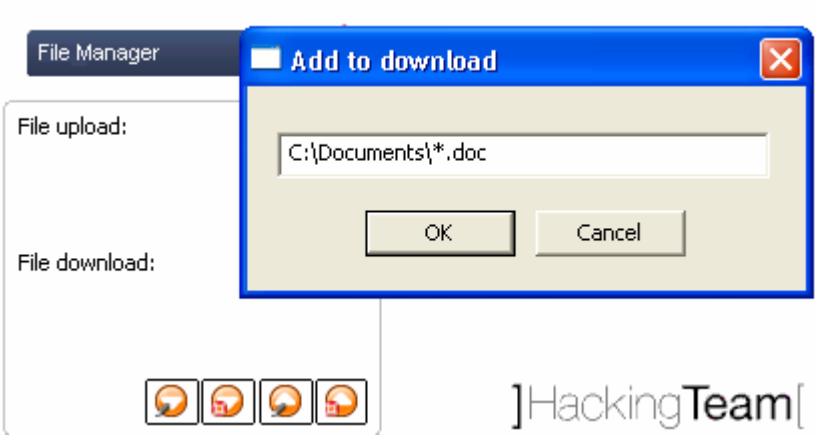
- Print agent
  - Intercetta tutte le pagine stampate dal PC
- Snapshot agent
  - Intercetta le schermate grafiche del PC

- Keylog agent
  - Intercetta i tasti in modo contestuale (nome programma, nome finestra), è supportato il sistema Unicode (lingue non occidentali,etc.)
- Url agent
  - Intercetta gli URL acceduti dal browser del PC
- Files agent
  - Intercetta i nomi dei file aperti/modificati/cancellati (con la possibilità di download successivamente)
  - Matching dei nom per inclusione ed esclusione (*.doc tranne *win*)
- Skype agent
  - Intercetta tutte le comunicazioni voce tramite Skype comprensivo di nome e numero telefonico (ver.2.0-2.5-3.0 pienamente supportate)
  - Il sistema e' in grado di isolare l' audio unicamente prodotto da Skype, non vi sono alterazioni dei dati attraverso sistemi di playback esterni (es.mediaplayer)
- Crisis agent
  - Quando attivato inibisce il funzionamento della sincronizzazione e dell' esecuzione di comandi

4.13. File transfer

Il sistema permette il trasferimento in upload e download di file.

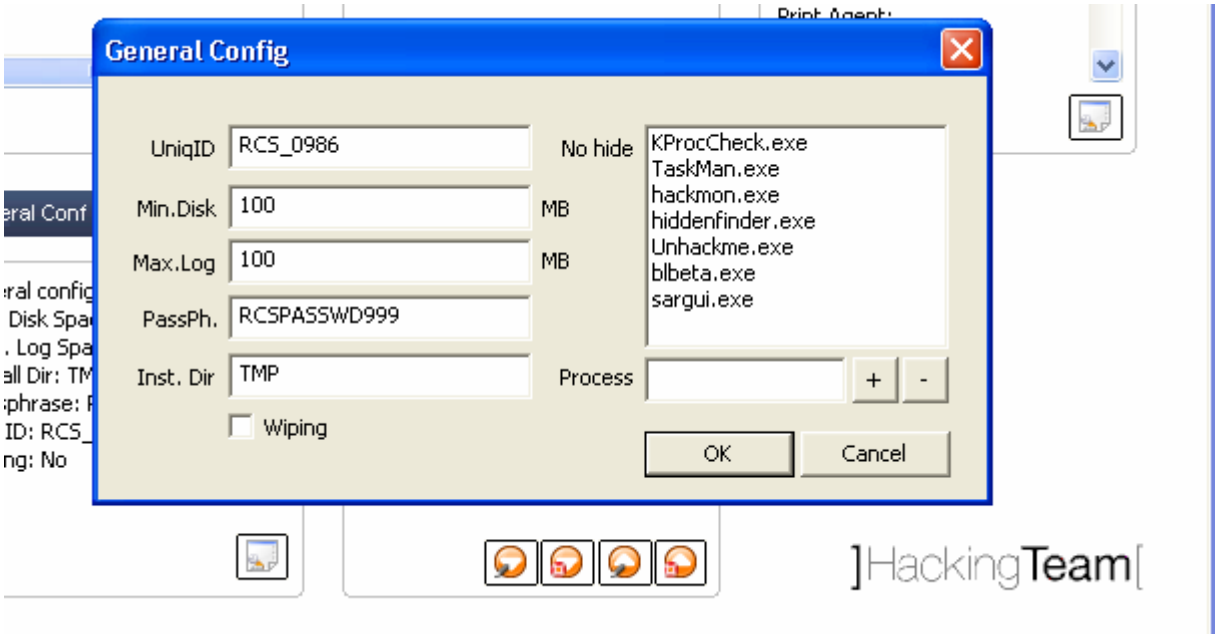
La gestione del file transfer avviene mediante apposito pannello di controllo in HCM4.



Il sistema di download supporta le variabili ambiente di windows e supporta le wildcard, vedi immagine di cui sopra. Il sistema di upload e' relativo alla directory random invisibile creata dal sistema al momento dell' installazione.

4.14. Configurazione generale

Caratteristiche di funzionamento più generali al sistema vengono impostate mediante apposito pannello di controllo di HCM4.



E' possible identificare alcuni parametri di configurazione:

- ID di identificazione
- Minima quota disco
- Massima dimensione log
- Password di cifratura
- Directory temporanea
- Wiping dei files
- Processi dai quali non mimetizzarsi

4.15. Protezione del codice

Al fine di massimizzare la protezione dello strumento e di garantirne la massima invisibilità e resistenza anche in presenza di analisi offline mediante strumenti di reverse engineering e decompilazione, RCS è dotato di meccanismi allo stato dell' arte.

La generazione del codice è polimorfica, il payload è cifrato e polimorfico, la directory e i nomi dei file sono random, sono state introdotte tecniche di anti-reversing.

4.16. Evoluzioni previste

Entro 2 mesi dalla consegna è previsto il rilascio della versione sul nuovo sistema operativo Windows Vista Home Edition Basic;

Entro 6 mesi dalla consegna è previsto il rilascio della versione sul nuovo sistema operativo Windows Vista Premium e Professional;

Entro 12 mesi dalla consegna è previsto il rilascio del modulo VoIP sui sistemi:

- Microsoft Live Messanger
- Altri sistemi “mainstream” quali ad esempio: Yahoo Messanger with voice, Google talks, Zfone/PGP Phone)

Al momento della consegna del prodotto è previsto un periodo da concordare di training on the job che consentirà all’utente l’utilizzo in autonomia del prodotto, tale training avrà una durata prevista pari a massimo 3gg uomo.

4.17. Hardware

La fornitura è comprensiva di 2 server aventi le seguenti caratteristiche:

Front end di ascolto:

- Dell PowerEdge 840
  - Intel Dual Core
  - 2GB Ram
  - 2 x 160GB SATAII hot-swap
  - Controller SAS/SATA integrato con supporto RAID1 (mirroring)
  - LCD 17" + scheda video
  - Tastiera, Mouse

Back end DB:

- Dell PowerEdge 840
  - Intel Dual Core
  - 2GB Ram
  - 3 x 160GB SATAII hot-swap
  - Controller PERC5i integrato con supporto RAID5
  - LCD 17" + scheda video
  - Tastiera, Mouse

Tre anni di Garanzia Dell Standard su entrambi I server

5. RESPONSABILITÀ

Sarà responsabilità di Hacking Team garantire il corretto funzionamento del software ed intervenire per la correzione di eventuali malfunzionamenti o aggiornamenti che si rendano necessari, restano esclusi gli sviluppi per l'utilizzo su Sistemi Operativi diversi da quelli attualmente previsti e di seguito indicati. Sarà responsabilità del Cliente garantire l'accesso ai locali preposti, nonché la disponibilità del personale necessario durante le attività previste dalla presente fornitura.

6. OFFERTA ECONOMICA

6.1. Costo a voi riservato

Condizione valida qualora il cliente proceda all'acquisto entro e non oltre il 31/06/2007.

Descrizione	Quantità	Costi
Licenza RCS Modulo Base (Win2K / Win XP / Win NT / Win 2003	1	**€ 40.000,00**
Manutenzione per 24 mesi Modulo Base (20% licenza sw)	1	**€ 10.000,00**
Licenza RCS Modulo VoIP	1	**€ 40.000,00**
Manutenzione per 24 mesi Modulo VoIP (20% licenza sw)	1	**€ 8.000,00**
Licenza RCS modulo Hacking resources	1	**€ 16.000,00**
Manutenzione per 24 mesi Modulo Hacking resources	1	**€ 4.000,00**
Harware	2	**€ 2.000,00**
Manutenzione Harware del costruttore	2	**Compresa**
Totale fornitura		**€ 120.000,00**

(importi al netto di IVA)

N.B.

- La licenza RCS si intende relativa ad un'unica ad un'unica Control Station (centrale d'ascolto), senza limitazione sul numero di PC oggetto di intercettazione.
- La fornitura include l'hardware adeguato al funzionamento dello strumento in offerta
- La manutenzione decorre dalla data di consegna dei singoli moduli

6.2. Documentazione Utente

La documentazione tecnica relativa al prodotto è compresa nei servizi sopra esposti.

Con cadenza trimestrale verrà rilasciato al committente un rapporto attestante le attività di testing svolte dal fornitore per garantire il corretto funzionamento del prodotto rispetto alle caratteristiche descritte.

6.3. Piano di manutenzione

Il servizio offerto dall'assistenza tecnica di Hacking Team con la sottoscrizione del contratto di fornitura e manutenzione prevede, limitatamente alla durata del contratto stesso, di mesi 24 (ventiquattro) dalla consegna del software, le seguenti prestazioni:

1. diritto a ricevere a titolo gratuito gli aggiornamenti relativi alla versione del software in licenza d'uso, in particolare sono garantite per la durata del contratto le caratteristiche intrinseche al sistema così come richiamate nel capitolato tecnico.
2. diritto a ricevere a titolo gratuito hotfix o patch relativi a malfunzionamenti del prodotto.
3. assistenza telefonica e via e-mail, da parte del personale di Hacking Team, accessibile durante le normali ore lavorative della settimana. Dal lunedì al venerdì dalle 9 alle 18,00.

7. CONDIZIONI DI FATTURAZIONE E PAGAMENTO

La presente offerta ha validità per ordini pervenuti entro il 31/05/2007.

La fatturazione dei prodotti avverrà come segue:

- Alla consegna comprensiva di canone di manutenzione

I pagamenti si intendono tutti a 30gg d.f. – a mezzo bonifico bancario

Hacking Team S.r.l.

Gabriele Parravicini
Responsabile commerciale