SECURITY DIVISION
Security & Intelligence Services

Security Division

Protocollo: SD.OffShore.20100201031730.2.0.0

DESCRIZIONE: **Servizi Intelligence OffShore**

DATA APERTURA: 01/02/10 **DATA CHIUSURA:** 05/02/10

Analisi *Esigenze* e offerta *OffShore*

Security Division ha studiato un pacchetto da proporre alle aziende che operano in quelle nazioni dove la privacy è normalmente violata dalle istituzioni o dove le infrastrutture, anche temporanee, non possano garantire un alto livello di sicurezza.

Paesi come la Cina, dove le intercettazioni sono praticamente automatiche e il governo installa dei malware nelle piattaforme di chi entra in rete (i computer vengono venduti già infettati), sono ricche di società che avrebbero bisogno di questo servizio.

Il gruppo propone la consulenza per la realizzazione dell'infrastruttura e la formazione, i servizi invece sono offerti gratuitamente ai nostri clienti che usufruiscono del pacchetto consulenziale.

Il pacchetto "**Off Shore**" prevede consulenza su:

1 - Assessment, verifica delle vulnerabilità simulando un attacco reale verso le piattaforme del cliente, utilizzando le più sofisticate tecniche conosciute e non, onde prevenire i principali attacchi usati da hacker e governi ostili.

2 - Bonifica da malware e cimici informatiche. Non una semplice ricerca di virus, ma il riconoscimento di trojan e bot che mai verranno riconosicuti dagli antivirus e l'analisi della memoria del sistema e delle chiamate al kernel e ai driver per bloccare ogni collegamento sospetto.

3 - Hardenizzazione del sistema, l'insieme di modifiche e contromisure per rendere la macchina immune ai principali attacchi, cambiando il registro, l'avvio dei servizi e l'accesso a driver e kernel. Saranno inseriti anche dei filtri e un sistema antivirus/malware personalizzato.

4 – Cifratura Disco che renda impossibile il recupero dati anche con la forensica. Il disco viene modificato perchè contenga apparentemente dati casuali al suo interno, in modo da sembrare vuoto o corrotto. In verità i dati saranno cifrati e ripristinabili solo tramite una chiave. Sarà fornita anche una chiavetta USB cifrata per i Documenti.

5 - Disco remoto cifrato all'estero (Panama/Russia)

Per archiviare i propri documenti e reperirli da qualsiasi postazione in modo sicuro. Sarà possibile rendere sicuro un server dedicato ai backup, dove ognuno avrà il suo spazio cifrato e inaccessibile agli altri (inaccessibile pure a noi), per le copie di sicurezza e i documenti.

6 – VPN su server estero (Panama/Russia) per navigare senza essere intercettati e senza filtri sui siti visitati.

Il cliente dal suo computer si collegherà al nostro server che si collegherà a un secondo server (e volendo a un terzo e un quarto) e il nostro server finale si collegherà a internet. La connessione tra il cliente e il nostro server è cifrata e non intercettabile, così come la connessione tra un server e l'altro della rete VPN. Inoltre in questo modo saranno aggirati i filtri di contenuti imposti da alcuni governi (vedi Cina, Emirati Arabi, etc.), in quanto il nostro server sarà collocato in un paese senza alcuna limitazione.

7 - Email GPG e **server di posta** cifrato all'estero (Panama/Russia)

Per autenticare il mittente dei messaggi di posta e impedire che siano leggibili da altri. Installazione del software necessario sulle macchine del cliente e formazione sul funzionamento le best practices.Collocazione di un Server di posta sicuro, all'estero (a Panama o in Russia) con SMTPS/POP3S e Webmail HTTPS.

8 - Chat cifrata per comunicare con noi o con i partner. Messaggistica, anche su rete MSN, Yahoo, Skype, ma cifrata. Sarà comunque possibile comunicare con un medio livello di sicurezza anche con i contatti che usino MACOSX ma che non abbiano usufruito del servizio. La comunicazione con client non cifrati è comunque garantita.

7 - Formazione per i dipendenti delle società che usufruiscono del servizio.

E' necessario che i nostri formatori vadano in sede per spiegare il semplice utilizzo della nostra tecnologia.

8 - Policy comportamentali scritte per l'utilizzo sicuro delle piattaforme in oggetto (Security Division). Servono principalmente per mantenere il livello di sicurezza impostato dai nostri tecnici, in riferimento alla formazione già ricevuta.

PACCHETTI OPZIONALI

9 - Chiavetta Internet per potersi collegare ovunque senza utilizzare le reti locali (partner a seconda del paese). La chiavetta su rete GSM/GPRS/UMTS/HSDPA/HSUPA permette infatti di evitare gli attacchi chiamati Man in the Middle (MiM), in cui un ascoltatore si immette tra chi manda i dati e chi li riceve, intercettandoli.

Chiunque sia nello stesso ufficio non sarebbe in grado di intercettare le comunicazioni del cliente, in quanto viaggianti su una rete esterna all'ufficio (quella cellulare appunto).

10 - Connessione SAT. La connessione satellitare, per i più esigenti, rende praticamente impossibile l'intercettazione, in quanto il computer si collegherebbe direttamente col satellite e questo diretamente col suo ufficio o con una nostra connessione in Europa. Anche se il cliente si dovesse trovare in un paese ostile, la connessione non sarebbe mai collegata alla rete internet nazionale, ma viaggerebbe direttamente verso il satellite in modo cifrato. Provare a intercettare le connessioni satellitari richiede non solo competenze, ma anche costosissime apparecchiature, che non garantiscono comunque di riuscire a decifrare il messaggio.

11 – Telefono cellulare cifrato. La comunicazione crittata a 256bit è considerata non ancora decifrabile per la maggiorparte dei governi. Anche le comunicazioni normali non cifrate verso telefoni comuni sono garantite.

11 – SIM anonima. Ricaricabile autonomamente (vodafone inglese, ricaricabile con ricariche italiane) o tramite noi (anche altre compagnie e altri paesi).

12 – Carta credito ricaricabile anonima. Ricaricabile alle poste o ricaricabile da noi (carta al portatore).

13 – Società anonima europea, americana o offshore.

14 – Conto in banca anonimo offshore, legato alla società anonima.

Andrea Bodei per **Security Division Srl**