5824

POLIZIA DI STATO

COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI PER L'UMBRIA
Via Mario Angeloni 72 - Perugia
Tel. 075/5001703 - 5011967 Fax.075/5000655
poltel.pg@poliziadistato.it
Settore Operativo

Prot. 1975/07– PG4 Perugia, 19 Novembre 2007

OGGETTO: Procedimento Penale 9066/07 R.G.N.R. mod.21.
Analisi file di Log.

Il sottoscritto Ass.te GREGORI Mirko, in servizio presso la Squadra di P.G. di questo Compartimento, riferisce alla S.V. quanto segue:

In riferimento al decreto di acquisizione file di log notificato al gestore FastWeb, l'analisi dei file di log ha permesso di individuare le seguenti riscontri:

L'analisi al momento effettuata nel periodo temporale, che và dal 01/11/2007 alle ore 18:00 fino alle ore 08:00 del 02/11/2007, è stata condotta mediante l'esame degli indirizzi IP definiti di "*IP di destinazione*", i "bite" scambiati e la porta "*porta di destinazione*". Tale elemento risulta fondamentale per individuare il server e/o Client P2P (*Utente internet che utilizza programmi specifici per lo scambio di file*) e grazie alla porta di destinazione è possibile stabilire il servizio che tale IP è in grado di erogare.

L'attività effettuata verso la rete internet è prevalentemente del tipo P2P, infatti numerosissime, sono le connessioni stabilite e dalle quali si evince un traffico dati elevato su tali software.

Analisi della navigazione web:

L'analisi della navigazione è stata condotta filtrando le porte di destinazione 80 (porta standard dei server web),443 (porta che permette la navigazione crittografata con lo

standard SSL, utilizzata ad esempio per servizi di e-commerce e tutti i servizi di autenticazione di parti riservate dei siti internet compreso l'accesso alla posta elettronica da pagina web).

Tale traffico risulta essere di esigua quantità ed in alcuni casi ripetuto costantemente nel tempo come ad esempio l'indirizzo IP 209.85.135.91 appartenente ad dominio Google risultano connessioni ogni 30 minuti, per un trasferimento dati di pochi bite.

Tale tipo di attività può essere attribuita alla presenza dell'applicazione per la visualizzazione delle pagine web (Web Browser) che in maniera autonoma richiama tale connessione.

Ulteriore verifica è stata effettuata sulle porte di destinazione in uso alla posta elettronica e chat non riscontrandone la presenza di traffico.

L'analisi tuttavia deve essere considerata parziale in quanto il file oggetto di analisi è composto da numerosissime connessioni a servizi non standard in fase di valutazione, ed inoltre verranno condotte operazioni relative alla configurazione, del Web Browser e dei programmi applicativi che utilizzano la rete internet, utilizzata dal sollecito.

In allegato è presente l'estrapolazione dei contatti individuato nei file di log sulle porte 80 e 443(porte utilizzate dal programma di navigazione web).