**MODELLO QUERELA PERSONA GIURIDICA IN CASO DI PAGAMENTO DEL RISCATTO (MOD. 1)**

**ILL.MA**

**PROCURA DELLA REPUBBLICA**

**PRESSO IL TRIBUNALE DI \_\_\_\_\_\_\_\_\_\_\_\_**

**\*\*\***

**ATTO DI DENUNCIA QUERELA**

**\*\*\***

Il sottoscritto \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, nato/a a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ prov. \_\_\_\_ il \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, residente a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ prov. \_\_\_\_, in via \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, n. \_\_\_\_, in qualità di rappresentante legale della

Società/Ditta \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(di da ora la Società), con sede in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_) \_\_\_\_\_\_\_ (cap) , via \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Codice Fiscale . \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Partita IVA \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Contatti

Telefono \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mail 1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mail 2 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PEC \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

con il presente atto propone

**DENUNCIA QUERELA**

nei confronti di ignote persone, per i reati di estorsione ex art. 629 c.p., accesso abusivo a sistema informatico ex art. 615-ter c.p., frode informatica ex. art. 640-ter c.p., e per ogni altro reato che la S.V. Ill.ma vorrà ravvisare nei fatti di seguito esposti.

\*\*\*

**Premessa**

Lo scrivente, unitamente ai dipendenti della Società, è utilizzatore del dispositivo elettronico/personal computer

marca\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, modello \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

sistema operativo \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ versione \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Tale strumento viene adoperato principalmente per motivi professionali che riguardano la gestione degli affari della Società e in particolar modo per tutte le attività che solitamente necessitano l'impiego di un elaboratore elettronico per la loro gestione, come: redazione di documenti digitali, navigazione on line, editing di contenuti informatici, ecc.. Proprio in ragione della destinazione del dispositivo, all’interno dello stesso, sono presenti numerosi contenuti riservati che sono destinati ad un utilizzo e alla consultazione privata del sottoscritto o delle persone abilitate da quest’ultimo ad accedervi.

\*\*\*

1. In data, xx mese anno, il sottoscritto (indicare eventuale persona diversa e suo ruolo in seno ala Società) stava utilizzando il proprio personal computer/dispositivo per navigare in internet sulla pagina http://www.nomesito.it. Durante la sessione di navigazione, è stato riscontrato un problema per il quale è stato necessario scaricare un file che, come suggerito dalla stessa pagina internet che stavo visitando, avrebbe risolto il piccolo inconveniente rilevato.
2. Lo scrivente, che non ha una conoscenza approfondita di informatica e solitamente si limita ad utilizzare tali apparecchi per attività abituali e non complesse, ha installato il predetto programma (All. 1) con la convinzione che questo servisse effettivamente per la corretta fruizione del servizio anzidetto.
3. In data, xx mese anno, il sottoscritto (indicare eventuale persona diversa e suo ruolo in seno ala Società) stava utilizzando il personal computer/dispositivo della Società per controllare l’avvenuta ricezione di messaggi di posta elettronica sulla casella [xxx@dominio.it](mailto:xxx@dominio.it) ( indicare casella di posta elettronica sulla quale è stato ricevuto il messaggio infetto). Durante tale operazione, è stata ricevuta una email, apparentemente inviata da \_\_\_\_\_\_\_\_\_\_\_\_\_\_( indicare tutti i dati del mittente del messaggio e specificare che tipo di file era allegato allo stesso), nella quale veniva consigliato di verificare il file allegato alla stessa.
4. Lo scrivente(specificare se persona diversa), che non ha una conoscenza approfondita di informatica, credendo che la mail fosse stata inviata effettivamente dal mittente indicato e ignorando la possibilità di poter prendere un virus con tale semplice operazione, ha provveduto all’apertura del file allegato alla email ricevuta (All. 1).
5. Tuttavia, non appena terminata l’operazione di apertura dello stesso, compariva sullo schermo una finestra (All. 2) all’interno della quale vi era un messaggio che mi comunicava che il mio personal computer era stato infetto da un “*ransomware*” (anche conosciuto come *cryptolocker*), che i miei file personali – contenuti all’interno della memoria del PC e nelle condivisioni di rete da esso raggiungibili erano stati criptati e che per poter nuovamente accedere a tali contenuti dovevo provvedere al pagamento di una somma di denaro attraverso una transazione da effettuarsi con il sistema di pagamento Bitcoin.
6. Occorre a questo punto specificare che per *ransomware* si intendono dei particolari tipi di virus informatici predisposti proprio per limitare l’accesso ai file o all’intero sistema del dispositivo che viene infettato. L’accesso ai file viene bloccato attraverso una o più chiavi di accesso che vengono comunicate dall’autore del virus (*Hacker*) al proprietario del computer solo in seguito al pagamento di una somma di denaro che, solitamente, avviene anch’essa per via informatica. Inoltre, tali programmi – essendo una derivazione di precedenti virus denominati *Trojan horse*, proprio per la somiglianza dell’attacco a quello del cavallo di troia- permettono all’intruso di poter accedere e modificare qualsiasi file contenuto all’interno del computer.
7. Invece, i bitcoin rappresentano il più famoso tipo di criptovaluta ovvero una rappresentazione digitale di valore[[1]](#footnote-1), decentralizzata[[2]](#footnote-2), basata sul peer-to-peer[[3]](#footnote-3), su una blockchain[[4]](#footnote-4) condivisa il cui trasferimento è basato sulla crittografia e le cui regole di emissione sono basate su un Algoritmo Open Source[[5]](#footnote-5). Tale tipo di moneta digitale, così come gli altri tipi di criptovalute esistenti, ha altresì alcune caratteristiche molto importanti tra le quali: la destinazione alla circolazione, la tracciabilità, la pseudonominatività e l’utilizzabilità come unità di conto. Tali caratteristiche rendono i bitcoin uno degli strumenti più utilizzati per effettuare pagamenti on-line di qualsiasi natura.
8. Ciò detto, successivamente alla visualizzazione di tale messaggio, effettivamente veniva verificato che non era più possibile aprire la quasi totalità dei documenti contenuti nel dispositivo, che seppur presenti risultano privi di contenuto intellegibile.
9. In ragione del fatto che uno o più file bloccati rivestivano una determinata importanza per la gestione della Società, decidevo di ottemperare alla richiesta di pagamento per rientrare in possesso dei documenti interessati.
10. A tal fine, riscontrando che la navigazione sui siti non era bloccata, veniva aperto un account “bitcoin wallet” sul sito http://xxxxx (specificare il sito di bitcoin exchanger utilizzato) per acquistare l’importo esatto di bitcoin richiesto come riscatto e, successivamente, provvedere al pagamento attraverso il sistema di pagamento digitale per ottenere la password di sblocco del dispositivo infettato.
11. Si specifica che il pagamento è stato effettuato attraverso il predetto portale e la transazione ha interessato: il mio indirizzo bitcoin (inserire se disponibile il Bitcoin address utilizzato per effettuare il pagamento – è un codice di 34 caratteri alfanumerici come ad esempio “19Ht4KU49M5KxXyEGzeaf67kTXRwWCnXxn”) e l’indirizzo Bitcoin di destinazione (inserire il codice alfanumerico di 34 caratteri comunicato nella schermata generata dal malware)

\*\*\*

Ritiene lo scrivente, che non vi sia dubbio che le condotte sopra evidenziate integrino perfettamente i reati prospettati. In particolare, relativamente al reato di estorsione previsto e punito dall’art. 629 c.p., risultano integrati tutti i suoi elementi costitutivi, quali: **la minaccia**, consistita nella prospettazione di non poter più entrare in possesso dei propri documenti e file contenuti nel PC, **la costrizione** intesa come coazione psicologia he si risolve nella compressione della libertà di autodeterminazione suscitata dalla paura del male minacciato e, in ultimo, **l’ingiusto profitto** in quanto l’utilità patrimoniale che l’agente si propone di realizzare con l’azione criminosa non è dovuta per legge che causa, di conseguenza, un **danno** di natura patrimoniale nel soggetto coartato.

Infatti, secondo l’interpretazione maggioritaria della giurisprudenza tale reato sussiste quando il malintenzionato **“*chiede ed ottiene dal derubato il pagamento di una somma di denaro come corrispettivo per l'attività di intermediazione posta in essere per la restituzione del bene sottratto, in quanto la vittima subisce gli effetti della minaccia implicita della mancata restituzione del bene come conseguenza del mancato versamento di tale compenso..*” [[6]](#footnote-6)**

Inoltre, il fatto che attraverso l’installazione di tale software il malintenzionato sia riuscito ad accedere al contenuto del mio personal computer e impostare una password per impedire l’apertura di tutti i file in esso contenuti, integra chiaramente la condotta di accesso abusivo a sistema informatico ex art. 615-ter. che si configura nella **“condotta di colui che accede o si mantiene in un sistema informatico o telematico protetto, violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare dell’elaboratore per delimitarne oggettivamente l'accesso.”[[7]](#footnote-7)**

Ed ancora, in tema di frode informatica ex art. 640-ter c.p. si ravvisano gli elementi dell’**alterazione ed intervento sui dati**  effettuati attraverso il programma installato che ha dato libero accesso all’hacker di operare sui medesimi e per il quale ha ottenuto un **ingiusto profitto**. In tema, la costante interpretazione della giurisprudenza osserva che **“*Il reato ex art. 640-ter c.p. prevede due distinte condotte; la prima consiste nell'alterazione, in qualsiasi modo, del funzionamento di un sistema informatico o telematico; la seconda è rappresentata dall'intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un dato sistema informativo o telematico. Tale ipotesi, finalizzata pur sempre all'ottenimento di un ingiusto profitto con altrui danno, si concretizza in un'illecita condotta intensiva, ma non alterativa del predetto sistema*.”[[8]](#footnote-8)**

\*\*\*

Per tutti i motivi sopra esposti, il sottoscritto

**CHIEDE CHE**

la S.V. Ill.ma voglia penalmente perseguire gli ignoti autori di tali condotte per il reati di estorsione, accesso abusivo a sistema informatico e Frode informatica rispettivamente ex artt. 629, 615ter e 640-ter c.p. e per ogni altro reato che la S.V. Ill.ma vorrà ravvisare in relazione ai fatti su esposti;

**CHIEDE**

di essere avvisato, ai sensi dell’art. 408 c.p.p., in caso di richiesta di archiviazione e, ai sensi dell'art. 406 comma 3 c.p.p., in caso di eventuale richiesta di proroga del termine per le indagini preliminari.

**ALLEGA**

i seguenti documenti:

1. Copia digitale della mail o del file in cui è presente il malware.
2. Screenshot della schermata di Cryptolocker con le istruzioni per sbloccare il dispositivo (in alternativa allegare il file TXT solitamente nominato "DECRYPT\_INSTRUCTIONS.TXT", contenente all'interno la URL personale dove ci sono le indicazioni sul riscatto e l'indirizzo bitcoin sul quale versare il riscatto).
3. Screenshot della schermata relativa all’operazione di pagamento bitcoin in cui sia visibile l’indirizzo di destinazione.

Città, lì XX Mese Anno

**Nome Cognome**

1. Rappresentazione di una quantità non emessa da autorità (centrale o pubblica), non necessariamente collegata a moneta a corso legale che può essere usata come mezzo di scambio o trasferita, immagazzinata o commercializzata elettronicamente. [↑](#footnote-ref-1)
2. Sistema basato sull’assenza di un emittente, di un amministratore ovvero di un gruppo di controllo e su filosofia “open source”. [↑](#footnote-ref-2)
3. Rete che non possiede nodi gerarchizzati sotto forma di client o server fissi, ma un numero di nodi equivalenti che possono fungere sia da *client* che da *server* verso gli altri nodi della rete ed ognuno in grado di avviare ovvero completare una transazione. [↑](#footnote-ref-3)
4. Registro distribuito incrementale delle transazioni, liberamente accessibile e basato sul consenso decentralizzato. [↑](#footnote-ref-4)
5. Programma informatico aperto e pubblico che contiene un numero determinato e finito di istruzioni per la realizzazione del sistema [↑](#footnote-ref-5)
6. Cass. pen. Sez. II, Sentenza n. 6818 del 31-01-2013, (rv. 254501) [↑](#footnote-ref-6)
7. Cass. pen. Sez. II, Sentenza n. 52680 del 20-11-2014, (rv. 261548) [↑](#footnote-ref-7)
8. Cass. pen. Sez. II, Sentenza n. 13475 del 06-03-2013 [↑](#footnote-ref-8)