# Caso di Studio

# «Incident Response»

# FATTO 1

MENU CERCA la Repubblica ABBONATI GEDI SMILE | R ACCEDI

HOME CRONACA SPORT FOTO VIDEO ANNUNCI LOCALI CAMBIA EDIZIONE

IL CASO

## Trivulzio, attacco informatico "Hanno cancellato gli archivi"

di FRANCO VANNI

*A Ferragosto un presunto hacker ha manomesso i computer. Il misterioso episodio denunciato alla polizia postale. Persi rendiconti finanziari e documentazione sanitaria*

24 AGOSTO 2011 PUBBLICATO PIÙ DI UN ANNO FA 2 MINUTI DI LETTURA

Quarantotto ore per cancellare tutto. Due giorni per ripulire dai dati la rete informatica del Pio Albergo Trivulzio. L'attacco informatico è scattato a Ferragosto, con gli uffici chiusi. Dai pc e dai server della casa di riposo sono stati fatti sparire i documenti relativi alla contabilità, le schede cliniche dei pazienti, l'elenco del personale, i moduli di pagamento, l'agenda delle prenotazioni delle visite e tutto quello che riguarda il patrimonio immobiliare. La direzione del Pat ha fatto denuncia alla polizia postale, che su mandato della Procura indaga sull'autore e sulle motivazioni del blackout. Non si esclude che chi ha cancellato i dati abbia prima potuto copiarli. La Procura ha aperto un'inchiesta (al momento a carico di ignoti) per accesso abusivo a sistema informatico aggravato e danneggiamento informatico.

Chi è entrato nella memoria informatica del Pat aveva come obiettivo quello di

# FATTO 2

HOME

## Attacco hacker islamista al sito dell'aeroporto San Francesco


**Eleonora Sarri** 04 ottobre 2015

Attacco hacker di presunta matrice islamista al sito dell'aeroporto di Perugia. Nel giorno di San Francesco, patrono d'Italia e santo a cui è dedicato lo scalo aeroportuale, collegandosi al portale dell'aeroporto (http://www.airport.umbria.it/) compare l'immagine di Tunisian Fallaga Team con tanto di combattente islamico e messaggio in inglese. In sottofondo anche

# Fasi

## Incident management workflow

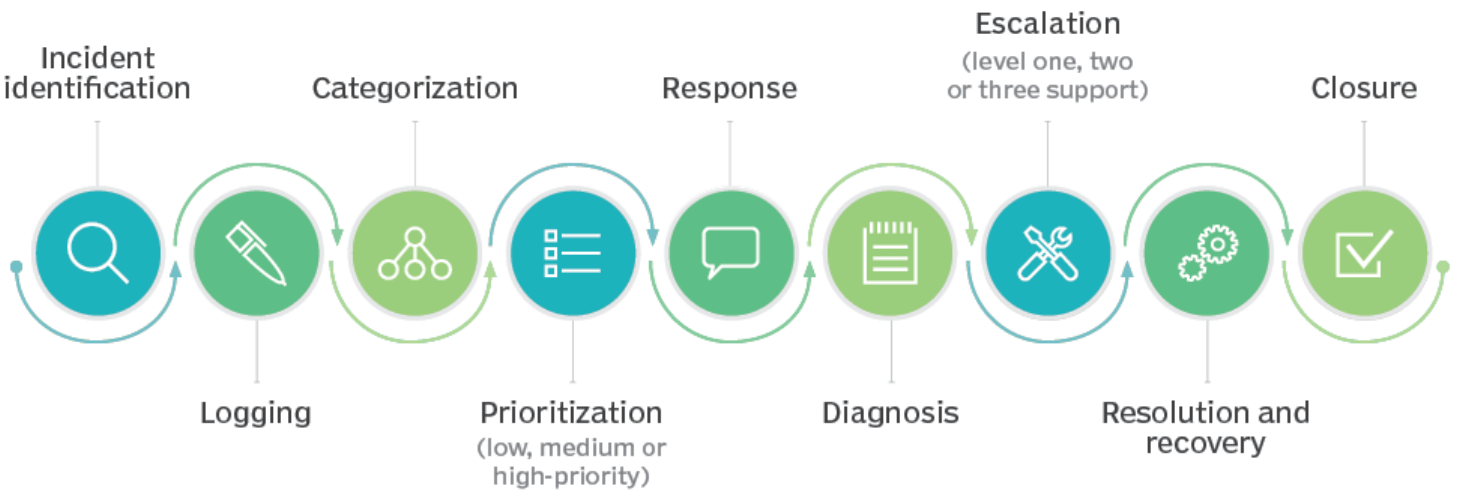


ILLUSTRATION: FIREOHEART/GETTY IMAGES; TRETER/ADOBE STOCK

# I FASE

## Identificazione dell’incidente

# Identificazione dell’incidente

Che sta succedendo?

# Identificazione dell’incidente

Abbiamo accesso a tutto il sistema informatico o dobbiamo interessare altri amministratori di rete o responsabili?

# Identificazione dell’incidente

Fermare l’attacco se è in corso

# II FASE

## Categorizzazione dell’incidente

# Categorizzazione dell’incidente

È un attacco mirato o casuale?

# Categorizzazione dell’incidente

Individuare tutti i dispositivi coinvolti

# Categorizzazione dell’incidente

Prima stima dei danni

# III Fase

## Risposta all’incidente

# Risposta all’incidente

Verifica della presenza di backup non compromessi

# Risposta all’incidente

Verifica degli accessi dai firewall per identificare un eventuale punto di ingresso

# Risposta all’incidente

Se viene individuato il punto di accesso, provvedere ad una copia fisica della memoria del dispositivo, compresa la RAM

# IV Fase

## Soluzione dell’incidente

# Soluzione dell’incidente

Ripristino del sistema dai backup

# Problemi

# Problemi

1) Non sono stati fatti backup
2) I backup sono compromessi
3) i dati sono stati criptati
4) Non si hanno privilegi di amministratore
5) Non si hanno supporti dove memorizzare le copie fisiche degli HD
6) I sistemi non prevedono desktop virtualizzati
7) L'attaccante è ancora presente con sistemi di C&C
8) Il responder va in panico
9) L'amministratore di rete non è raggiungibile
10) Il sistema informatico non è ben strutturato

# Problemi

1) Il sistema non riesce a tornare on line
2) Sono stati compromessi dispositivi che si collegano a distanza
3) I log dei firewall sono compromessi
4) È stata usata come ingresso proprio la macchina dell’amministratore di rete
5) È finito il caffè

# V Fase

## Analisi dell’incidente

# Analisi dell’incidente

1) Analisi dei file di log dei firewall
2) Analisi dei dispositivi sicuramente compromessi
3) Verifica dell’architettura della rete
4) Verifica della tenuta dei backup
5) Analisi di tutti i dispositivi in rete per verificare eventuali trojan
6) Verifica dell’efficienza nella risposta all’incidente

# TRIVULZIO

Con parti tratte da:

S. ATERNO, F. CAJANI, G. COSTABILE, D. CURTOTTI

***CYBER FORENSIC ED INDAGINI DIGITALI***

*Giappichelli Editore, 2021*

# TRIVULZIO

Sulla richiesta di data 5.10.2012 (depositata in data 9.10.2012) formulata dal Pubblico Ministero di applicazione della misura coercitiva della custodia cautelare in carcere per il seguente reato:
p. e p. dagli ***artt. 81, 61 n° 11, 615 ter commi 1, 2 e 3 c.p.*** perché, nella qualità di dipendente del Pio Albergo Trivulzio (PAT) e con abuso di relazione di ufficio, collegandosi – con la *user name* delfo2000@yahoo.it – ai servizi di anomizzazione di PROXPN attraverso l'IP 85.88.202.118 (assegnato staticamente al F. dalla società Lineacom Srl), ottenendo a suo favore l'assegnazione dei seguenti IP ad opera di PROXPN

**collegamento inizio fine**
**13 ago 2011 16.37 16.37 213.179.212.76**
**13 ago 2011 16.45 16.46 213.179.212.76**
**13 ago 2011 16.47 17.30 213.179.212.76**
**13 ago 2011 19.09 21.37 109.203.115.89**
**13 ago 2011 22.45 02.31 109.203.115.71**
**14 ago 2011 02.39 03.02 213.179.212.122**
**14 ago 2011 03.05 03.29 173.231.157.74**
**14 ago 2011 03.42 04.23 109.203.115.66**
**14 ago 2011 19.33 20.51 109.203.115.109**
**14 ago 2011 21.11 21.42 109.203.115.109**
**14 ago 2011 22.10 22.11 213.179.212.70**
**14 ago 2011 23.47 23.47 213.179.212.69**
**15 ago 2011 01.38 01.47 173.0.5.51**

ed utilizzando il programma *Team Viewer,* accedeva abusivamente da remoto con ID 846389785 al sistema informatico del PAT protetto da misure di sicurezza.
Con le aggravanti che: dal fatto è derivato il danneggiamento di tale sistema informatico, l'interruzione parziale del suo funzionamento nonché la distruzione dei dati e delle informazioni ivi contenute; trattasi di sistema informatico relativo alla sanità pubblica e comunque di interesse pubblico.

# TRIVULZIO

**ORIGINE dell'INDAGINE**

Il procedimento ha origine dal devastante attacco informatico sferrato da anonimi *hacker* in prossimità del Ferragosto 2011 (le successive indagini hanno acclarato che detto attacco ha avuto inizio il 13.8.20114 alle ore 14.37 ed è proseguito fino alle 11.14 del 15.8.2011, giorno di Ferragosto) contro il sistema informatico del **PAT** (**Pio Albergo Trivulzio**), meglio noto ai cittadini milanesi come "BAGGINA" (dal nome del periferico quartiere in cui sorge dal lontano 1910) e formalmente e giuridicamente inserito nell'**Azienda di Servizi alla Persona – Istituti Milanesi Martinitt e Stelline e Pio Albergo Trivulzio** *(con sede a Milano in via Marostica n°8)*, ente pubblico senza scopo di lucro le cui finalità si realizzano precipuamente nei settori dell'assistenza socio-sanitaria.

# TRIVULZIO

Le **indagini** condotte fin da subito (sul punto si evidenzia che già in data 18.8.2011 il PM di turno sentiva a
s.i.t. G.E. – direttore dei sistemi informativi del PAT – che aveva sporto denuncia contro ignoti in data 17.8.2011 presso la Polizia di Stato – Compartimento Polizia Postale e delle Comunicazioni per la Lombardia
– in seguito alla rilevata intrusione nella rete informatica aziendale) dalla **Polizia Postale di Milano** sotto la
direzione ed il coordinamento della **Procura della Repubblica di Milano** sono consistite inizialmente nell'**assunzione a s.i.t.** dei vari soggetti a vario titolo coinvolti nella gestione di detto sistema informatico e
nel **sequestro** in data 18.8.2011 della **postazione informatica** di M.G. (dalla quale sembrava essere partita
l'intrusione), nonché di un secondo computer utilizzato dalla squadra tecnica del PAT come *file server* (ossia
come *repository* di *file*), e nella **conseguente analisi forense degli stessi HD**, per poi proseguire in data
6.9.2011 nell'**acquisizione di documentazione** inerente l'organizzazione complessiva del servizio informatico
del PAT.

# TRIVULZIO

Con nota del 29 settembre 2011 la PG restituiva **l'analisi forense degli HD sequestrati il 18 agosto scorso,**
**ed in particolare del computer in uso a M.** (dal quale si ritiene sia avvenuta l'intrusione), analisi che confermava come
**l'attacco sarebbe avvenuto dal PC del M. (PATHD02), utilizzando il programma *Team viewer*, con l'ID**
**846389785;**
**l'intrusione è iniziata nel primo pomeriggio del 13 agosto (dalle ore 14.37), protraendosi almeno sino alle**
**11.14 di Ferragosto;**
**l'intruso possedeva probabilmente la *password* di accesso mancando tracce su altre modalità di accesso**
**al sistema;**
**l'intruso ha cercato di nascondere le tracce dell'attacco cancellando il log di *Team Viewer* con la modalità**
**"salva", cioè aprendo il *file* di *log*, cancellando quanto vi era memorizzato e poi salvando il file vuoto.**

# TRIVULZIO
# Indagine

*Ascoltate le persone che potevano fornire elementi utili a ricostruire il quadro della organizzazione generale del PAT e i dettagli sui momenti prossimi alla scoperta del fatto, in particolare gli appartenenti al gruppo di gestione informatica (fra i quali non vi era F.), visionato direttamente tutti i luoghi interessati dalla vicenda – in specie quelli ove erano fisicamente allocati server e computer – verificato quindi lo stato dell'infrastruttura informatica e le modalità con le quali quest'ultima era stata annichilita, gli operatori di questo Compartimento accertavano l'inesistenza di una qualsiasi traccia di natura classica. L'attacco al sistema informatico del PAT era stato infatti realizzato esclusivamente per mezzo di vie telematiche e quello era l'unico cammino sul quale poteva forse trovarsi qualche elemento utile.*

# TRIVULZIO
# Indagine

*Il problema inizialmente emerso era che prima di uscire dal sistema l'autore dell'azione criminosa, dimostrandosi accorto, astuto e soprattutto preparato, si era premurato di cancellare anche le tracce informatiche del suo accesso abusivo allorché si allontanava dall'infrastruttura del PAT. Queste tracce sarebbero state le "impronte" lasciate dal suo passaggio e solo queste avrebbero potuto in qualche modo tradirlo. Di qui la cancellazione, non solo dei dati, ma anche la distruzione parziale del sistema, per renderlo inagibile ed evitare che una sua ricomposizione potesse far emergere queste "impronte".*

# TRIVULZIO
# Indagine

*non è da sottacere la circostanza che l'analisi tecnica dell'azienda L. Service (che aveva all'epoca un contratto di assistenza con il PAT) a seguito del suo intervento in modalità IRT (incident response team) dopo l'attacco informatico, non rivelò dati utili per le indagini.*

# TRIVULZIO
# Indagine

*Il compartimento Polizia Postale ha avuto l'idea di* ***provare a ricomporre la configurazione degli hard disk che costituivano l'ossatura dell'infrastruttura, cioè ricostruire le memorie informatiche del PAT compromesse dall'attacco per potervi poi ricercare eventuali tracce estranee alla normale conduzione aziendale, riconducibili cioè all'attacco****. In altre parole restaurato il tracciamento delle operazioni informatiche giornalmente condotte nel sistema informatico nel PAT si sperava di poter isolare e identificare così una traccia riferibile all'intrusione esterna con la quale è stato sferrato l'attacco*

# TRIVULZIO
# Indagine

***il principale risultato della complessa analisi condotta sugli hard disk del PAT fu la scoperta che per accedere all'infrastruttura informatica l'ignoto attaccante era "transitato" attraverso il computer di M.G.****, uno dei tecnici impiegati presso l'azienda pubblica col compito di gestire la manutenzione del sistema informatico. In quanto tale, M. era (è) in possesso di tutti i privilegi di amministratore, quindi di tutte le password.*

*Accedere alla postazione di M. significava quindi avere la chiave di accesso a tutti i varchi del sistema, per le varie macchine fisiche e virtuali componenti dell'infrastruttura, raggiungibili attraverso una semplice connessione RDP (Remote Desktop Control), un protocollo Microsoft incluso nei pacchetti commercializzati dall'azienda americana*

# TRIVULZIO
# Indagine

*P.M. – E lì invece solo TeamViewer.* ***Per cui quando lei dice "Ah, ma io non sapevo se TeamViewer l'avevano messo all'UTC o all'orario italiano", le dico che nell'analisi di M. la Polizia Giudiziaria dice che l'analisi... che TeamViewer è stato utilizzato a partire da un orario UTC ad un altro orario UTC, e inizia alle 14.37****. Io guardo la sua relazione e lei dice "****No, c'è un problema, perché io ho rilevato che il programma inizia alle 16.37", ma guarda caso sono giusto 2 ore in più, 14.37 UTC, 16.37 orario italiano****.*
*Se lei avesse fatto la conversione era 14.37 dice Garrisi, […]. Sì o no?*
*C.T. DIFESA – mi sono un attimo perso sinceramente.*

# TRIVULZIO
# Indagine

*C.T. DIFESA – Sì sì, ho capito, ma allora quello che dovrei fare in questo momento è prendere i dati di quello che chiamo "Analisi Garrisi", spostarli di sei ore, e vedere che forme si rappresentano.*
*P.M. – no,* ***lei doveva sincronizzare l'orario del computer che lei ha analizzato con quello invece dei dati di Garrisi****, visto che Garrisi fa riferimento a dei dati che ha ricevuto da Proxpn li ha già analizzati e le dà l'indicazione di orario.* ***Lei arriva e dice "No, attenzione, è tutto sbagliato perché le 16.37 è fuori dalla Timeline di Garrisi", le chiedo: ma non è che forse lei non ha sincronizzato la sua analisi con quella di Garrisi prima di fare le valutazioni?*** *Io dico, prima di fare le valutazioni, io sto ancora adesso analizzando sul suo metodo, sto facendo tutte domande sul suo metodo, quali atti ha ricevuto, se ha fatto da solo o con l'indagato, se ha fatto correttamente la conversione del fuso orario. Domande sul metodo del Consulente, perché, ripeto, poi dopo le Parti discuteranno sui risultati. Quindi visto che alla Procura e alla Polizia Giudiziaria interessava TeamViewer, e lei dice "Attenzione TeamViewer è 16.37", le rifaccio la domanda perché è chiaro al Giudice però io vorrei una risposta se sì o no: lei ritiene di aver fatto correttamente la conversazione del fuso orario e quindi questa discrepanza che lei ha rilevato è rimproverabile ad un suo errore di metodo, sì o no?*

# TRIVULZIO
# Indagine

*C.T. DIFESA – a dire il vero la mia analisi doveva riuscire a sopperire anche ad eventuali errori di localizzazione nella tempistica, perché mi ero molto... faccio molto affidamento sul fatto che se anche ci fossero stati orari differenti... fusi orari differenti le forme che rappresentano i momenti in cui c'erano un tipo di attività e l'altra attività combaciassero spostate ma...*
*P.M. – la domanda è semplice. Su TeamViewer, che era uno degli elementi fondamentali, poi le farò altre domande e l'Avvocato può fare le altre domande sul resto, però io le dico, su questa discrepanza, che guarda caso evidenzia TeamViewer fuori dalla Timeline della Polizia Giudiziaria,* ***le ripeto per la terza volta e deve rispondere o sì o no****, forse è un suo errore di metodo che non ha correttamente sincronizzato il fuso orario della sua analisi orario italiano con il fuso orario di Garrisi?*

# TRIVULZIO
# Indagine

*C.T. DIFESA – prima di risponderle, in cui naturalmente è evidente che possa aver fatto un errore di localizzazione del tempo, va detto che TeamViewer è eseguito alle 16.37, mentre qui si sta parlando di orari che inizierebbero alle otto di mattina, che anche sommandoci 6 ore arriveremmo alle 14.00.*
*P.M. – Le ripeto, Dottor .... lei ha analizzato gli atti e non può dire che quella annotazione fa riferimento a TeamViewer, perché quella annotazione a cui lei fa riferimento fa riferimento all'accesso alla Proxpn, l'annotazione a cui fa riferimento a TeamViewer è l'altra che lei ha sotto occhio, se è la prima volta che la vede mi dispiace per il Consulente, però in quella annotazione si dice che l'orario di TeamViewer è dalle 14.37 UTC, quella è il suo atto di riferimento.*
*C.T. DIFESA – ho capito, eh...*
*P.M. –* ***c'è un errore, sì o no, di metodo?***
*C.T. DIFESA –* ***sì.***

# TRIVULZIO

Con nota del 29 settembre 2011 la PG restituiva **l'analisi forense degli HD sequestrati il 18 agosto scorso,**
**ed in particolare del computer in uso a M.** (dal quale si ritiene sia avvenuta l'intrusione), analisi che confermava come
**l'attacco sarebbe avvenuto dal PC del M. (PATHD02), utilizzando il programma *Team viewer*, con l'ID**
**846389785;**
**l'intrusione è iniziata nel primo pomeriggio del 13 agosto (dalle ore 14.37), protraendosi almeno sino alle**
**11.14 di Ferragosto;**
**l'intruso possedeva probabilmente la *password* di accesso mancando tracce su altre modalità di accesso**
**al sistema;**
**l'intruso ha cercato di nascondere le tracce dell'attacco cancellando il log di *Team Viewer* con la modalità**
**"salva", cioè aprendo il *file* di *log*, cancellando quanto vi era memorizzato e poi salvando il file vuoto.**

Email :

raffaele.garrisi@poliziadistato.it