Tribunale di Bologna
Sezione Lavoro

Procedimento R.G. n. 1234/2021

Marco Rossi
vs
Azienda s.p.a.

Consulenza Tecnica nell'interesse del dott. Marco Rossi

Prof. Pico Dellamirandola

19 gennaio 2024

INDICE

1 SCENARIO GENERALE

Questa relazione ha lo scopo di evidenziare diversi aspetti critici della documentazione presentata da controparte in questo procedimento.

Pur basandosi solamente sulla documentazione presentata da controparte, non si possono escludere scenari interpretativi del tutto differenti da quelli prospettati da controparte ai fini di questo procedimento. In altri termini, i fatti in oggetto potrebbero essere interpretati altrimenti da come sono mostrati da controparte.

Si intende evidenziare come siano state trascurate diverse verifiche che avrebbero potuto consentire ulteriori scenari interpretativi completamente differenti. Questo non è stato fatto da controparte, in base ai documenti presentati, che sembra abbiano lo scopo di «dimostrare» una tesi precostituita senza accertare la completezza dello stato dei fatti, o quantomeno di escludere possibili ulteriori scenari.

In altri termini, si ritiene che basandosi sui documenti di controparte siano possibili anche conclusioni completamente differenti da quelle sostenute.

L'argomento di base è che *Azienda s.p.a* non abbia presentato documenti a dimostrazione inconfutabile delle proprie tesi.

1.1 Notazione tipografica

In questa relazione sono presenti elementi di testo che rimandano ad altro[1]; tali elementi sono inscritti in un rettangolo; ad esempio i titoli dell'indice e le note a pié di pagina. Il seguente § 3 – che è il rimando alle conclusioni – è un ulteriore esempio di rimandi ad un'altra sezione dello stesso documento.

2 SUI DOCUMENTI PRESENTATI A AZIENDA S.P.A.

2.1 Sui docc 1 del 2 marzo e 2 del successivo 30 marzo 2021

Le contestazioni originarie, contenuta nella «contestazione disciplinare» , doc 1 del 2 marzo 2021, possono essere sintetizzate come segue[2]:

- « *. . . tentativo di avvio di software, su una postazione di lavoro, di un software* ***potenzialmente*** *malevolo*»[3]

1. Tali elementi, detti *ipertestuali*, quando vengono "cliccati" portano direttamente ad uno dei seguenti: ad un'altra parte dello stesso documento, ad un altro documento, oppure ad un documento web.
2. L'enfasi espressa in carattere neretto è stata aggiunta dallo scrivente
3. Primo capoverso della prima pagina del documento.

- infrazione di policy aziendali sull'uso di strumenti tecnologici – scarico e avvio dell'installazione di software non autorizzato abusando dei privilegi di amministratore di sistema – con l'aggravante che il software in oggetto fosse **potenzialmente** malevolo [4]
- «*All'uso improprio dello strumento, si aggiunge dunque l'elemento del danno,* ***rimasto solo potenziale*** *. . .* » [5]

È importante evidenziare che si menziona solamente software *potenzialmente* malevolo, mentre non è affatto dimostrato che sia software *attualmente* malevolo. Anzi, come dichiarato in udienza da Vittorio Martini, dipendente di Azienda dove opera nel settore della sicurezza[6]
«ADR: Per l'azienda non ci sono stati danni».
Di conseguenza si può concludere che alla prova dei fatti il software in analisi **non si è rivelato malevolo**. In altri termini, come confermato anche da controparte, l'operato attribuito a Marco Rossi **non ha cagionato alcun danno ad Azienda**, evidentemente **non si può dedurre che il codice in oggetto contenesse malware**.

2.2 Sulla relazione di Sherlock Consulting

La relazione di Sherlock Consulting – d'ora in avanti Sherlock – così come è stata richiesta da Azienda, appare orientata solamente a verificare le ipotesi del committente, senza analizzare nella sua completezza lo stato dei fatti; tanto che si legge nel primo capoverso dell'Introduzione, a pag 4 di 23:
«In data 23.03.21 la società Azienda S.p.A. (di seguito "il committente") ha chiesto all Sherlock Consulting Srl di provvedere all'acquisizione forense e alla successiva analisi dei *log* (registri) della piattaforma Microsoft Defender for Endpoint utilizzata dalla società, in particolare relativi alle attività compiute nel seguente asset aziendale:
Hostname: h810484
Periodo di interesse: dalle 00:00 del 15.02.2021 alle 23:59 del 15.02.2021»

Appare evidente che l'incarico di Azienda a Sherlock fosse quello di acquisire forensicamente soltanto i *log*, per un solo giorno, dello specifico programma di sicurezza. Questa richiesta ha portato a trascurare e rendere successivamente inservibile[7] qualsiasi altra

4. Ultimo capoverso della prima pagina e i due seguenti.
5. Alla fie del secondo capoverso della seconda pagina.
6. Come si legge nel «Verbale della Causa» del 9 marzo 2022, al penultimo capoverso.
7. La mancata cristallizzazione del contenuto del disco del computer a ridosso dei fatti contestati inficia l'attendibilità di eventuali risultati rinvenuti successivamente, e comunque non ancora cercati alla data odierna. Potenzialmente quel computer potrebbe essere stato alterato in molti modi e sicuramente gli usi successivi hanno modificato quantomeno i file temporanei.

informazione contenuta nel computer in uso al dott. Rossi. Solamente l'acquisizione forense completa del disco del computer avrebbe potuto cristallizzare quanto in esso contenuto, in modo da poterlo analizzare nella sua interezza[8]. L'incarico dato a Sherlock, invece, ignorava dell'analisi dell'intero contenuto del computer, ma richiedeva solo quella di una sua piccolissima parte.

Inoltre, è evidente che Azienda non possa essersi basata sugli esiti della perizia di Sherlock per decidere del licenziamento del dott. Rossi, dato che questa è stata commissionata due giorni dopo il licenziamento e consegnata quasi nove mesi dopo.

Come si legge nella relazione di Sherlock i software in oggetto sono costituito dai seguenti programmi:

1) *dogecoin-1.14.2-win64-setup-unsigned.exe*
2) *dogecoin-1.14.2-win32-setup-unsigned.exe*
3) *multidoge-0.1.7-windows-setup.exe*

Questi software sono di tipologia *open source* e può essere reperito al sito di *GitHub*[9] agli indirizzi indicati anche nella relazione di Sherlock. Il sito GitHub è un sito che gode di alta reputazione e che funge da distributore di software cosiddetto a *codice aperto*.

È importante osservare ben due software su tre non erano noti ad Azienda all'epoca del licenziamento, tanto che sono emersi solo a seguito dell'analisi di Sherlock, che è stata prodotta nel dicembre 2021, ossia nove mesi dopo il licenziamento. Nella «contestazione disciplinare» e nel successivo «provvedimento disciplinare» è menzionato solamente il software *dogecoin-1.14.2-win32-setup-unsigned.exe*

Il software *dogecoin-1.14.2-win32-setup-unsigned.exe* non è mai stato eseguito sul computer in uso al dott. Rossi, come si legge nella contestazione disciplinare alla nota della prima pagina. L'affermazione contenuta nella stessa nota riguardo alla possibilità che questo software *potesse essere* vettore del malware «Trojan Uwasson» è una afferma-

8. Questo *modus operandi*, è raccomandato da tutti gli standard e le più diffuse pratiche di informatica forense.

9. Come si legge in wikipedia, è «Il sito è principalmente utilizzato dagli sviluppatori, che caricano il codice sorgente dei loro programmi e lo rendono scaricabile dagli utenti. Questi ultimi possono interagire con lo sviluppatore tramite un sistema di issue tracking, pull request e commenti che permette di migliorare il codice del repository risolvendo bug o aggiungendo funzionalità. Inoltre Github elabora dettagliate pagine che riassumono come gli sviluppatori lavorano sulle varie versioni dei repository»

zione di carattere potenziale, probabilmente basata solo su considerazioni generali[10]. Il software non risulta essere stato analizzato dal programma di sicurezza per verificare la presenza di malware, quindi l'esecuzione è stata impedita solamente sulla base di *possibilità* e non di *evidenze*. In altri termini, esiste in rete una versione di *dogecoin-1.14.2-win32-setup-unsigned.exe* infettata da un malware, pertanto il programma di sicurezza ha impedito l'esecuzione di un software con quel nome, a prescindere, senza verificare se quello specifico software fosse effettivamente infettato.

A seguito dell'acquisizione forense solo di alcuni file e non dell'intera memoria di massa del computer, non è più possibile verificare in modo incontrovertibile niente altro oltre agli stessi *log*, ad esempio l'eventuale presenza di malware di tipo *rootkit*. Non è più possibile verificare se del malware fosse presente nella memoria di massa del computer oppure se c'era ed è stato successivamente cancellato; tantomeno non si può più stabilire con certezza se quello specifico file *dogecoin-1.14.2-win32-setup-unsigned.exe* contenesse malware di qualche tipo. Ancora, non si può più verificare la presenza e lo stato al momento dei fatti di: eventuali *rootkit*[11], eventuali cookie, estensioni dei browser, storia del browser, timeline degli eventi, ...

Occorre evidenziare che un *utente* di un personal computer, ossia una entità identificata da un account e da una password, non coincide necessariamente con la *persona* titolare di quella utenza. Ad esempio, un'altra persona o un software malevolo possono utilizzare una utenza per compiere azioni pur non essendo quella persona. Correttamente la relazione di Sherlock indica l'utenza e non la persona nella prima riga della tabella di pagina 7: «accesso ... avviato dall'utente Marco.Rossi». Questo non vuol dire che necessariamente la persona Marco Rossi abbia compiuto quelle azioni, ma solo che il suo utente (ossia l'entità identificata con le sue credenziali) lo ha fatto. Ad esempio un *rootkit* potrebbe avere eseguito delle azioni in luogo della persona.

---

10. La nota dice testualmente: «Operazione del tutto necessaria dato che è riportato sul web che il programma il cui lancio era stato bloccato è stato rilevato più volte essere vettore del Trojan Uwasson». Una ricerca dello scrivente sul Web ha prodotto due occorrenze dello stesso testo che segnala una variante *infetta* ai siti https://coin.fyi/news/dogecoin/doge-wallet-trojan-uwasson-a-is-affected-by-dogecoin-1-14-2-win64-setup-uns-i1mdvj e https://www.reddit.com/r/dogecoin/comments/i1mdvj/doge_wallet_trojan_uwassona_is_affected_by/ entrambi visitati l'ultima volta in aprile 2020.

11. Nel sito del famoso software anti-malware Kaspersky, all'indirizzo https://www.kaspersky.it/blog/che-cosa-sono-i-rootkit/645/, (ultima visita aprile 2020) si legge la seguente definizione «Rootkit è un tipo di malware disegnato per attaccare computer e eludere i sistemi di sicurezza. Il rootkit permettere all'hacker di installare una serie di strumenti che gli danno accesso al computer da remoto. In genere il malware si nasconde in un punto profondo del sistema operativo ed è studiato in modo tale da non essere rilevato dalle applicazioni anti-malware e dai principali strumenti di controllo e sicurezza.»

Come si rileva anche nelle conclusioni della relazione di Sherlock, al punto 2 della pagina 21 di 23, che nell'intervallo complessivo di mezz'ora i software in oggetto sono stati: scaricati, provati con alterni risultati ed infine disinstallati. Il tempo in cui il software *dogecoin-1.14.2-win32-setup-unsigned.exe* è restato installato, senza alcun rilievo da parte dell'anti-malware, è di circa dieci minuti[12].

Occorre notare che alcune delle conclusioni proposte da Sherlock appaiono fuori contesto: i punti a, b, c, nulla hanno a che fare con lo scopo dichiarato della relazione, invece sono una risposta all'atto di impugnazione presentato dal dott. Rossi. Tale atto è datato 12 novembre 2021, ossia più di 8 mesi dopo l'incarico a Sherlock da parte di Azienda.

La conclusione 4, invece appare compatibile con un eventuale furto di credenziali.

Non sono riportate analisi di ulteriori parti del sistema, ad esempio del registro, per accertare quali fossero gli altri programmi installati.

3 CONCLUSIONI

Non si può sostenere che il software in oggetto contenesse malware. Tanto da non aver cagionato alcun danno, come conferma la stessa Azienda. Comunque non risulta una scansione di quel software, che è stato bloccato in base ad una *presunzione* e non ad un *accertamento* da parte del programma di sicurezza.

Le attività contestate al dott. Rossi sono durate complessivamente mezz'ora, all'interno della quale un software è stato installato per 10 minuti, senza essere mai stato eseguito perché bloccato dal programma di sicurezza.

Non è stata neanche presa in considerazione l'ipotesi di un furto di credenziali e si confonde l'utenza di un computer con la persona fisica.

Quanto illustrato nella relazione di Sherlock è sicuramente compatibile con le tesi di Azienda, ma allo stesso tempo non esclude altre possibili spiegazioni dell'accaduto, ad esempio la presenza di un *rootkit*, che non sono state nemmeno indagate. Il *modus operandi* di Azienda ha addirittura reso inattendibili eventuali analisi in tal senso.

Bologna, il 19 gennaio 2024.

prof. Pico Dellamirandola

12. Si faccia riferimento alle pagg. 11 e 12 di 23 dove l'installazione è indicata alle 11:26 e la disinstallazione alle 11:36.