Proc. N. 21245/16 RGNR

TRIBUNALE DI ROMA

SEZIONE DEI GIUDICI PER LE INDAGINI PRELIMINARI

Ufficio 37

ORDINANZA DI APPLICAZIONE DELLA MISURA CAUTELARE

DELLA CUSTODIA IN CARCERE

(art. 272 e ss. c.p.p.)

Il Giudice, dott. Maria Paola Tomaselli,

Visti gli atti del procedimento penale N. 21245/16 nei confronti di:

- OCCHIONERO Giulio, nato a Roma [redacted] residente a Londra (GB), ma di fatto domiciliato a Roma in via [redacted]

- OCCHIONERO Francesca Maria, nata a Medford (USA) [redacted] residente a Londra (GB), ma di fatto domiciliata a Roma in via [redacted]

INDAGATI

A) per i reati di cui agli artt. 81 cpv, 110, 56, 494, 615 ter, commi 1°, 2° n. 3) e 3°, 617 quater, commi 1°, 4° n.1, 617 quinquies co. 1° 3e 2° (con rif all'art. 617 quater comma 4° n.1) c.p. perché, in concorso fra loro e al fine di procurare a sè stessi ed altri un vantaggio, con più atti esecutivi di un medesimo disegno criminoso, accedevano abusivamente alla casella di posta elettronica, protetta da misure di sicurezza, [redacted] in uso allo Studio legale dell'Avv. Ernesto Stajano, quindi da tale casella, sostituendo illecitamente la propria all'altrui persona, ponevano in essere atti idonei, diretti in modo univoco ad indurre in errore il Dott. Francesco DI MAIO, responsabile della Sicurezza della società ENAV S.p.A.; in particolare inviavano all'ENAV S.p.A. un messaggio di posta elettronica contenente un allegato malevolo (virus informatico EyePyramid), che una volta

auto – installato nel sistema informatici dell'ENAV S.p.A., avrebbe permesso di accedere abusivamente al relativo sistema informatico, contenente informazioni e dati relativi alla sicurezza pubblica nel settore dell'aviazione civile, nonchè di intercettarne le comunicazioni informatiche e/o telematiche al suo interno.

In Roma, acc.to il 28 aprile 2016

B) per il reato di cui agli artt. 81, 110, 615 ter, commi 1°, 2° n. 3) e 3°, 615 quater, comma 2. in relazione al n. 1 dell'art. 617 quater, 617 quater, commi 1°, 4° n.1, 617 quinquies, co. 1° 3e 2° (con rif all'art. 617 quater comma 4° n.1) c.p. ed art. 167 commi 1 e 2, d.lgs. n. 196 del 2003, perchè in concorso fra loro e con più atti esecutivi di un medesimo disegno criminoso, a scopo di acquisire indebitamente informazioni, atti, documenti, anche di natura riservata e pertinenti alla sicurezza pubblica nonchè al fine di trarne per sé o per altri profitto o di recare ad altri un danno, accedevano abusivamente a caselle di posta elettronica protette dalle relative password di accesso, sia personali che istituzionali, appartenenti a professionisti del settore giuridico-economico nonchè a numerose autorità politiche e militari di strategica importanza,o di sistemi informatici protetti utilizzati dallo Stato o da altri enti pubblici (*istruzione.it, gdf.it, bancaditalia.it, camera.it, senato.it, esteri.it, tesoro.it, finanze.it, interno.it, istat.it, comune.roma.it, regione.campania.it, regione.lombardia.it, matteorenzi.it, partitodemocratico.it, pdl.it, cisl.it, unibocconi.it , ENAV S.p.A*), quindi, mediante l'installazione abusiva da remoto nei relativi sistemi informatici e telematici del malware Eyepiramid, idoneo a intercettare chiavi di accesso (username e password) e flussi di comunicazione telematica, acquisivano notizie che, nell'interesse politico interno o della sicurezza pubblica devono rimanere riservate e di cui in ogni caso è vietata la divulgazione, ovvero dati personali e sensibili relativi ad intestatari ed utilizz atori dei sistemi informatici e telematici violati

In Roma, dal 2012, condotte in corso di esecuzione.

Letta la richiesta di applicazione della misura cautelare della custodia in carcere avanzata nei confronti degli indagati dall' Ufficio del P.M.

GRAVI INDIZI DI COLPEVOLEZZA

Ritiene il giudicante di dover preliminarmente chiarire come la presente ordinanza ricalchi la dettagliata e puntuale richiesta avanzata dall' ufficio del P.M. dovendo condividersi sia il metodo con il quale si è proceduto alla ricostruzione della presente vicenda , sia l' analisi tecnica delle risultanze investigative .

Si è, quindi , preferito distinguere nell' ambito della esposizione la fase della genesi dell'indagine , avuto riguardo alla segnalazione trasmessa dal dott. Francesco Di Maio , responsabile della sicurezza della società ENAV s.p.a. , corredata dall' analisi tecnica effettuata dalla società Mentalt Solutions s.r.l. [1] ,per poi evidenziare lo sviluppo dell' attività investigativa posta in essere da operatori di P.G. dotati di una particolare competenza tecnica . Il contesto probatorio emerso a seguito degli accertamenti svolti , che hanno beneficiato della piena collaborazione delle autorità statunitensi , ha trovato , infine , un pieno riscontro nell' esito dell' attività di monitoraggio effettuata. Le operazioni di intercettazione telematica e telefonica svolte hanno , infatti , da un canto confermato la riconducibilità all' Occhionero Massimo ed alla sorella delle condotte contestate e dall' altro hanno consentito anche di assistere all' attività dai medesimi posta in essere volta ad occultare le loro responsabilità mediante la distruzione dei file oggetto dell' illecito accesso .

Ed invero , come si vedrà in seguito , la captazione telematica dei computers in uso agli indagati ha consentito di verificare sia la disponibilità da parte degli stessi di alcuni dei files oggetto di esfiltrazione , sia la attività di inquinamento probatorio dai medesimi di seguito realizzata , mentre l' intercettazione dei colloqui intercorsi tra di loro ha evidenziato come essi fossero gli autori dell' illecita condotta .

Genesi dell' indagine

In data 1.03.2016 il Dott. Francesco DI MAIO, Responsabile della Sicurezza della società ENAV S.p.A., infrastruttura critica nazionale convenzionata con il CNAIPIC della Polizia Postale, segnalava l'avvenuta ricezione di un messaggio email contenente un allegato malevolo, da lui ricevuto in data 26.01.2016 ed apparentemente inviato dallo studio legale del Prof. Ernesto Stajano.

In particolare, la detta mail era risultata sospetta perché costui non aveva mai avuto relazioni dirette con il Prof. Stajano o con il suo studio legale. Pertanto, anziché visualizzarla e scaricarne

[1] Società che opera specificamente nel settore della sicurezza informatica !!!!!!!!!!!!!

l'allegato, provvedeva opportunamente ad inviarlo per l'analisi tecnica alla società *MENTAT Solutions S.r.l.*, che opera specificamente nel settore della sicurezza informatica e della malware analysis.

Dall'analisi dei dati tecnici a corredo del messaggio di posta elettronica in argomento (*header*) effettuata dalla P.G. , veniva così riscontrato che questo era stato inviato alle ore 10:43:51 del 26.01.2016, dall'indirizzo email mittente [redacted] utilizzando un mail server di proprietà della società *Aruba S.p.A.* avente indirizzo IP 62.149.158.90.

Gli accertamenti effettuati presso la società Aruba consentivano di accertare l'indirizzo IP utilizzato per inviare la mail, tramite il servizio di webmail: 37.49.226.236. **(vds. Allegato 1 dell'informativa Polizia Postale CNAIPIC del 26 ottobre 2016 in atti – alla stessa ci si richiamerà anche nei rimandi successivi).**

Tale indirizzo IP risultava appartenere ad un nodo di uscita della rete di anonimizzazione TOR **(vds. Allegato 2)**, stratagemma informatico che, di fatto, impedisce l'identificazione dell'effettivo utilizzatore.

Ad ogni modo, si accertava comunque che l'account mittente [redacted] faceva parte di una serie di account collegati a studi legali risultati compromessi a seguito di un'infezione informatica di cui meglio si parlerà in seguito. Ciò che conta sottolineare ora è che l'attaccante, proprio in virtù dell'infezione informatica, era in possesso della relativa password di accesso e ne aveva quindi la piena disponibilità.

Dalle analisi svolte era stato riscontrato come il file analizzato presentasse numerose analogie con un altro *malware* diffuso in precedenti campagne di *spear-phishing*[2], che personale dipendente della medesima società Mentat aveva già avuto modo di studiare nell'ottobre 2014, quando la società ENI S.p.A. era stata destinataria di messaggi "malevoli" al pari dell'Enav[3].

---

[2] lo spear-phishing è un particolare tipo di phishing (truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima al fine di carpire informazioni personali, dati finanziari o codici di accesso), realizzato ad hoc per colpire particolari individui o società.

[3] per un riscontro di ciò, si veda quanto dichiarato, in data 7.03.2016, da Federico RAMONDINO, titolare della società *MENTAT Solutions S.r.l.* escusso a sommarie informazioni al fine di acquisire informazioni più dettagliate circa l'esito dell'analisi del file malevolo, da lui effettuata per conto di ENAV S.p.A..

Lo stesso ha consegnato copia del report redatto nell'occasione su incarico dell'ENAV, (vds. allegato 3)

Più dettagliatamente, il *malware* rinvenuto nella mail indirizzata ad ENAV sarebbe corrispondente ad una recente versione di un virus denominato *EyePyramid*, già noto a partire dal 2008 in quanto all'epoca utilizzato in una massiccia e duratura campagna di attacchi informatici mirati, tramite la quale erano stati compromessi numerosi sistemi informatici appartenenti a società private e studi professionali.

L' EyePiramid, una volta installato, non solo garantisce all'attaccante il pieno controllo da remoto del sistema infettato, ma permette l'integrale sottrazione di documenti o di altre informazioni, incluse quelle riservate, senza che la vittima possa accorgersene.

Ciò perché l'esfiltrazione dei dati avviene mediante duplicazione e il successivo invio di file cifrati, con due distinte modalità di trasmissione:

- per i file di dimensioni molto grandi vengono utilizzati account di *cloud storage;*
- gli altri file vengono trasmessi in allegato a messaggi email inviati utilizzando account di posta elettronica aventi dominio dominio *@gmx.com*[4].

I tecnici MENTAT, grazie ad un software da loro appositamente realizzato, sono riusciti a decodificare i file trasmessi tramite email, mentre non sono stati in grado di decriptare gli altri.

Accertamenti tecnici

I tecnici della Mentat , partendo dall'allegato malevolo, **sono stati in grado di individuare un server punto di riferimento per il citato malware, ossia il c.d. server di *Command and Control* (C&C)[5] utilizzato per la gestione di tutti i sistemi informatici infettati e sul quale erano memorizzati i file relativi alla configurazione delle macchine compromesse dal medesimo virus EyePiramid[6], oltre a migliaia di documenti informatici abusivamente esfiltrati secondo la descritta modalità.**

4 Il dominio *gmx.com* è gestito dalla società statunitense *1&1 Mail & Media Inc.* con sede a Chesterbrook, (Pennsylvania).

5 un *Command and Control* (C&C) è un server utilizzato per controllare l'azione di un malware (e più in generale di una botnet), inviando file di configurazione alle macchine compromesse, o raccogliendo i dati da esse carpiti.

6 Sul server erano presenti 1133 file di configurazione, evidente indice di un egual numero di macchine compromesse.

La comune provenienza di tutti i malware che hanno infettato i sistemi che di seguito verranno citati è stata, in particolare, possibile grazie all'analisi tecnica del codice con cui è stato scritto il *malware* venuto alla nostra attenzione.

Infatti, in particolare dall'esame della libreria *MailBee.NET.dll*[7] utilizzata dal virus in questione per la sottrazione dei file tramite protocolli di posta elettronica e per la cattura di altre informazioni, sono emerse significative analogie presenti in tutte le versioni del *malware* analizzato, compresa quella in esame.

Così, fin dal maggio 2010, tutte le versioni del programma malevolo succedutesi nel tempo, fino al dicembre 2015, hanno sempre utilizzato la stessa licenza del componente MailBee.NET caratterizzata dallo stesso codice univoco identificativo *MN600-D8102T401003102110C5114F1T18-0E8CI*[8].

La licenza MailBee utilizzata dal malware è variata solamente nel dicembre 2015 quando, a seguito della richiesta effettuata dalla *MENTAT* di fornire le generalità del suo acquirente, la società *AFTERLOGIC Corporation* (produttrice delle componenti *MailBee.NET Objects* e destinataria della richiesta) ha ritenuto di dover notiziare a riguardo il proprio cliente.

Altro fatto, estremamente significativo, emerso dalle indagini è che, in una versione del virus diffusa alla fine del 2010, i dati carpiti dalle macchine compromesse venivano inviati ai seguenti indirizzi email: *purge626@gmail.com*[9], *tip848@gmail.com*, *dude626@gmail.com* e *octo424@gmail.com*. (*cfr. pag. 60 dell'allegato 3*).

Dall'analisi della MENTAT, emergeva poi che la versione attuale del malware reinoltrava il contenuto delle caselle email *@gmx.com* utilizzate per le descritte operazioni di data exfiltration, verso un account del dominio *hostpenta.com* (*gpool@hostpenta.com*), registrato sfruttando il servizio di *"whois privacy"* offerto dalla società statunitense *PERFECT PRIVACY, LLC*, con sede a Jacksonville (Florida), che oscura i dati identificativi del reale titolare del dominio.

---

7 La libreria *MailBee.NET.dll* è parte di un set di componenti commerciali chiamato *"MailBee.NET Objects"*, prodotto dalla società statunitense *AfterLogic Corporation*, con sede a Newark (Delaware).

8 Maggiori informazioni sono contenute nell'allegata relazione tecnica (*cfr. pagg. 52 e segg. dell'allegato 3*), alla quale si rimanda per una più dettagliata descrizione dell'analisi effettuata.

9 Questo sarebbe collegato a operazioni di controllo da parte di Bisignani nei confronti dell'onorevole Papa e delle Fiamme Gialle, nell'ambito dell'inchiesta relativa alla P4

Si accertava, inoltre che l'attività illecita di dossieraggio era stata attivata anni orsono e non era mai cessata, come testimonia il dato che, durante tutto il periodo di osservazione compiuto dagli operanti e dai loro ausiliari, il *malware* era oggetto di continua evoluzione[10].

In particolare, veniva riscontrato che nel mese di luglio vi sono state aggiunte due nuove classi, aventi il compito, rispettivamente, di creare *alert* in base ad una lista di parole chiave e di geolocalizzare la vittima in base all'indirizzo IP.

Significativa è soprattutto la prima delle due classi, in base alla quale nel momento in cui una delle keyword impostate veniva rinvenuta all'interno di un messaggio email ricevuto da una vittima, questo veniva automaticamente copiato ed inviato verso il server di C&C.

Inoltre, con una nuova forma di controllo da remoto dei sistemi informatici in uso alle vittime, denominata *"PolyCommand"*, era possibile inviare comandi alle vittime sotto forma di messaggi email.

Con ciò perseguendo l'ulteriore fine di mascherare ulteriormente la reale identità degli autori delle condotte illecite in oggetto: grazie a tale nuova funzionalità, difatti, alcune delle attività di gestione della *botnet* venivano effettuate utilizzando le stesse caselle delle vittime come origine delle richieste, come d'altronde avvenuto nel caso specifico della mail inviata all'ENAV dallo Studio legale Stajano.

Identificazione degli autori dei reati in epigrafe e gli ulteriori fatti-reato.

Come già evidenziato dalle indagini è emerso che, in una versione del virus diffusa alla fine del 2010, i dati carpiti dalle macchine compromesse venivano inviati ai seguenti indirizzi email: *purge626@gmail.com*[11], *tip848@gmail.com, dude626@gmail.com* e *octo424@gmail.com*. (*cfr. pag. 60 dell'allegato 3*) che da una ricerca effettuata su fonti aperte in rete (OSINT[12]) ed in particolare da fonti giornalistiche, risultavano essere già emersi nel luglio 2011, nel corso del procedimento penale c.d. P4, istruito presso la Procura della Repubblica di Napoli (P.M. Henry John Woodcock e Francesco Curcio). (cfr. allegato 3).

---

10 Ciò è emerso dalle analisi tecniche di eventuali nuove versioni del malware e della relativa infrastruttura di controllo. (vds. allegato 4)

11 Questo sarebbe collegato a operazioni di controllo da parte di Bisignani nei confronti dell'onorevole Papa e delle Fiamme Gialle, nell'ambito dell'inchiesta relativa alla P4

12 OSINT, acronimo di Open Source INTelligence, è l'attività di raccolta di informazioni mediante la consultazione di fonti di pubblico accesso.

Nello specifico tali indirizzi sarebbero stati riconducibili ad un'attività di esfiltrazione di dati e "dossieraggio" illecito effettuata con modalità del tutto analoghe[13] a quelle utilizzate dal malware oggetto del presente procedimento.

Da quanto narrato sinora si evince chiaramente come pur essendo stato riscontrato in pregresse vicende giudiziarie l'utilizzo del medesimo malwere, in precedenza non era mai stato possibile risalire al suo reale utilizzatore . Tuttavia erano già evidenti indizi gravi, precisi e concordanti che a utilizzare negli anni l'EyePiramid e i suoi aggiornamenti fosse stata sempre la stessa persona.

Riferimenti in tal senso erano ricavabili dalla circostanza che il codice fosse stato sempre lo stesso, con la logica conseguenza di poter ritenere che il malware fosse gestito nel tempo dalla stessa persona o organizzazione.

In altre parole, si deve ritenere che **l'acquirente della licenza *MailBee*, utilizzata all'interno del codice malevolo, corrispondeva alla persona che in questi anni gestiva il malware e ne aggiornava nel tempo le diverse versioni.**

Ebbene, è dal già citato dominio *hostpenta.com* che si è potuto identificare l'autore, o meglio gli autori, dei reati contestati.

Il dominio, infatti, risultava essere collegato con altri domini, tra i quali si evidenziano i seguenti: *enasrl.com*[14], *eyepyramid.com*, *marashen.com*, *occhionero.com*, *occhionero.net* e *westlands.com*.

Tutti questi domini risultano essere stati registrati utilizzando la medesima società statunitense (*Registrar: NETWORK SOLUTIONS, LLC.*) ed attualmente sfruttano il già descritto servizio di *"whois privacy"* offerto dalla società *PERFECT PRIVACY, LLC*, ma sono risultati tutti essere, a vario titolo, riconducibili a Giulio OCCHIONERO, o a società a lui collegate ove collabora con la sorella Francesca Maria OCCHIONERO.

Ulteriori accertamenti, effettuati per il tramite dell'F.B.I. statunitense presso la società *Afterlogic Corporation*, produttrice della licenza MailBee.NET Objects, permettevano di appurare che **la licenza relativa al componente utilizzato dal malware, dal maggio 2010 al dicembre 2015 risultava essere stata acquistata proprio da Giulio OCCHIONERO** (*cfr. allegato 5*

---

13 In entrambi i casi infatti il malware, dopo aver carpito i dati, li avrebbe cifrati e poi inviati a mezzo email.

14 **Si badi bene: il dominio *enasrl.com*, al pari di *hostpenta.com*, è presente all'interno del codice del malware.** EyePiramid è anche il nome del virus. La Westland è una società in cui operano i fratelli Occhionero (come emerge dal profilo Linkedin di Francesca Maria Occhionero).

dell'informativa del 28.04.2016). Per cui innegabile sembra essere, alla luce degli elementi sinora evidenziati, il coinvolgimento di quest'ultimo nelle attività delittuose descritte in epigrafe.

L'attività illecita di raccolta dati su persone e società risulta essere, poi, del tutto coerente con gli interessi personali di Giulio OCCHIONERO, così come scaturiscono dal contenuto delle conversazioni oggetto di intercettazione e dall' indubbio legame del medesimo con gli ambienti della massoneria italiana, in quanto membro della loggia *"Paolo Ungari – Nicola Ricciotti Pensiero e Azione"*[15] di Roma, della quale in passato ha ricoperto il ruolo di *maestro venerabile*, parte delle logge di Grande Oriente d'Italia.

L' attività di intercettazione

Ad ogni modo, pieni riscontri a quanto finora descritto, sono emersi dalle attività di intercettazione telefonica e telematica effettuate sulle utenze in uso a Giulio OCCHIONERO ed alla sorella Francesca Maria, come di seguito riportato nel dettaglio.

Nel corso dell'intercettazione telematica sull'utenza fissa numero [redacted] intestata a Giulio OCCHIONERO ed ubicata presso la sua abitazione, è stato infatti riscontrato come questi abbia la piena disponibilità e la gestione dei Server ove vengono memorizzati i file abusivamente prelevati dai P.C. oggetto di infezione.

Dall'analisi del traffico dati intercettato si è riusciti a ricostruire parte dell'architettura di rete utilizzate dagli indagati, identificando gli indirizzi IP e le funzionalità di alcuni dei server, oltre alla tipologia di comunicazioni effettuate. Per una completa descrizione dell'analisi effettuata si rimanda all'annotazione redatta dalla PG delegata. (**vds. allegato 6**).

In particolare, poi, è stata individuata la classica topologia di rete propria delle infrastrutture basate su server Microsoft, per la gestione di servizi quali: il DNS (per la risoluzione dei nomi di dominio), l'Active Directory attraverso un Domain Controller (con autenticazione di tipo Kerberos[16] ed accesso ai servizi di directory LDAP[17]), la condivisione di file con protocollo SMB e SMB2[18], i servizi di posta elettronica[19], oltre ad un server WEB.

---

15 Corrispondente alla loggia nr. 773 del Grande Oriente d'Italia, la più grande comunione massonica italiana.

16 Kerberos è un protocollo di rete per l'autenticazione tramite crittografia che permette a diversi terminali di comunicare su una rete informatica insicura provando la propria identità e cifrando i dati.

Si è inoltre appurato che tali server sono ubicati negli USA, e precisamente a Prior Lake (Minnesota) presso la società *"Dedispec LLC"* (server aventi indirizzi IP: **199.15.251.74, 199.15.251.75** e **199.15.251.76**) ed a Salt Lake City (Utah) presso la società *"Raw Data"* (server aventi indirizzi IP: **216.176.180.178, 216.176.180.180, 216.176.180.188** e **216.176.180.181**). Per una dettagliata descrizione delle funzionalità dei singoli server, si rimanda alla richiamata annotazione di cui all' allegato 6 .

Si evidenzia come tra i domini che risultano essere associati all'indirizzo IP 199.15.251.76 compaiano alcuni di quelli già emersi per essere associati al dominio *hostpenta* utilizzato dal malware *(cfr. pagg. 76 e segg. dell'allegato 3)*:

- *www.westlands.com, www.occhionero.info, www.wallserv.com, www.ennsrl.com, www.eurecoove.com, www.ayexisfitness.com, www.millertaylor.com* e *www.marashen.com.*

Tali domini inoltre, utilizzano tutti gli stessi server di posta, *mail.wallserv.com* e *mail2.wallserv.com*, aventi indirizzi IP 199.15.251.75 e 216.176.180.181, appartenenti quindi alla rete utilizzata da entrambi gli indagati.

Dall'analisi dei dati intercettati si è inoltre riusciti ad enumerare alcuni nomi di file e cartelle presenti sul server avente indirizzo IP 216.176.180.178 (risultato essere una replica di quello avente indirizzo IP 199.15.251.74 ed avente funzioni di Domain Controller e server DNS), che sono risultati essere riconducibili alle attività di creazione del codice malevolo[20].

Nel server in uso agli indagati è stata, inoltre, riscontrata la presenza delle cartelle *"hanger"* ed *"hostpenta"*, che corrispondono alle principali cartelle utilizzate per memorizzare i file esfiltrati dai sistemi target dell'infezione informatica; in particolare, il server avente indirizzo IP 216.176.180.180, basato su Microsoft SQL Server, funge da database e contiene, nella cartella *website*, sottocartelle relative a siti gestiti dagli indagati: *marashen.com, millertaylor.com, occhionero.info, wallserv.com, westlands.com* e *hostpenta.com*.

---

17 LDAP (acronimo di *Lightweight Directory Access Protocol*) è un protocollo per l'accesso a servizi di directory. Un server LDAP consente di effetmare operazioni di inserzione, cancellazione ed aggiornamento dei dati, come un database generico, ma è ottimizzato per effettuare operazioni di ricerca ed accesso alle informazioni.

18 SMB (acronimo di Server Message Block) è un protocollo usato principalmente per condividere file, stampanti, porte seriali e comunicazioni di varia natura tra diversi nodi di una rete. SMB2 non è altro che la versione 2 del protocollo SMB

19 La posta elettronica era gestita per mezzo dei protocolli SMTP ed IMAP (con utilizzo di cifratura tramite TLS).

20 descritte nella già citata relazione tecnica redatta dalla società MENTAT.

Ancora, al suo interno pure la cartella *data*, contenente un database in formato Access 2013 denominato *"InfoPyramid.accdb"* il cui contenuto è divenuto conoscibile grazie all'intercettazione telematica effettuata nei confronti degli indagati, sicché è stato possibile ottenere, sebbene in parte, quanto gli Occhionero avevano esfiltrato da sistemi target.

Un'approfondita analisi dei file contenuti ha consentito l'estrazione di una tabella nella quale sono riportati nomi, cognomi, indirizzi di posta elettronica, domini web, password, ecc.

Nello specifico si tratta di un elenco di 18327 username univoche, alcune delle quali (con precisione 1793) corredate da password, catalogate in 122 categorie denominate *Nick*, che indicano la tipologia di target (politica, affari, ecc.) oppure le iniziali dei primi due caratteri del loro nome e cognome.

Tale database contiene un elenco di persone attenzionate dagli indagati, che siano state oggetto di tentativi di infezione, più o meno riusciti.

In tal senso si ritiene che il campo *"LastSender"*, presente nella tabella, riporti l'ultimo indirizzo di posta elettronica utilizzato dagli indagati per veicolare il malware verso i target; mentre i campi *"Date"* e *"Previous"* starebbero ad indicare le date dei tentativi di infezione.

Tra le categorie (nick) più significative all'interno del database si evidenzia:

- *EYE:* raggruppa 144 diversi account utilizzati dall'indagato per gestire le dropzone[a] del malware (tale nick si ritiene derivi dal nome del malware: *EyePyramid*);
- *BROS:* raggruppa 524 differenti account di posta elettronica relativi a 338 nominativi univoci, verosimilmente appartenenti a membri della massoneria (in inglese Bros è l'abbreviazione di Brothers, ossia Fratelli).

Tra i nominativi presenti si evidenziano elementi di vertice della massoneria italiana, oltre a membri di logge del G.O.I. del Lazio, cui appartiene anche Giulio OCCHIONERO, come ad esempio:

Stefano Bisi *(Gran Maestro della Massoneria del Grande Oriente d'Italia)*

Franco Conforti *(presidente del Collegio dei Maestri Venerabili del Lazio)*

Luigi Sessa *(Gran Maestro Onorario del G.O.I.)*

Gianfranco De Santis *(ex Primo Gran Sorvegliante del G.O.I.)*

a La *dropzone* identifica lo spazio di memoria ove vengono inviati e raccolti i dati sottratti da un malware

Kristian Cosmi *(amico ed avvocato di Giulio Occhionero e membro della sua loggia)*

Massimo Manzo *(amico di Giulio Occhionero e membro della sua loggia)*

Giacomo Manzo *(membro del G.O.I del Lazio)*

Franco Conforti *(candidato a Presidente del collegio delle logge del Lazio)*

Antonio Fava *(candidato a Presidente del collegio delle logge del Lazio)*

Gregorio Silvaggio *(Ufficiale della G.d.F. ed ex Presidente del collegio delle logge del Lazio, ora "in sonno")*

Si ritiene che l'interesse che Giulio OCCHIONERO nutre nei confronti dei suoi fratelli massoni, possa essere legato a giochi di potere all'interno del Grande Oriente d'Italia , come d' altra parte testimoniato dal tenore di alcune conversazioni oggetto di captazione.

- *TABU*: che raggruppa diversi account e password con dominio *port.taranto.it*. (si ritiene possa essere l'abbreviazione di: TA=Taranto, BU=Business).

  Tale categoria assume particolare rilievo in quanto, come emerso da fonti giornalistiche (vds. allegato 7), la società Westland Securities riconducibile a Giulio e Francesca Occhionero, ha fornito consulenza al governo statunitense, in un'operazione commerciale per la costruzione di infrastrutture nel porto di Taranto. Conferma dell'impegno in tal senso avuto da Giulio e Francesca Occhionero emerge anche dal profilo *LinkedIn* della stessa Francesca Maria Occhionero. (vds. allegato 8)

- *POBU*: contenente 674 account, 29 dei quali corredati dalla relativa password. (si ritiene possa essere l'abbreviazione di: PO=Political, BU=Business). Tra gli account presenti nella lista e comprensivi della password se ne evidenziano alcuni con domini istituzionali *"interno.it"*, *"camera.it"*, *"senato.it"*, *"esteri.it"* e *"giustizia.it"*, o riconducibili ad importanti esponenti politici:

Nome	Cognome	Account	Note
Maurizio	Scelli	[redacted]	Parlamentare PdL XVI Legislatura
Sergio	De Gregorio	[redacted]	Senatore XV e XVI Legislatura (prima IdV e poi PdL)
Sergio	De Gregorio	[redacted]	

- Società private: *aceaspa.it, enel.it, eni.it, enav.it, finmeccanica.com, fondiaria-sai.it*

Per ciascuno dei domini sopra indicati, sono presenti numerosi account di posta elettronica, tra i quali figurano personalità di vertice delle società e delle istituzioni elencate, oltre che del mondo politico.

Sono presenti tra gli altri l'account Apple dell' ex Presidente del Consiglio On. Matteo Renzi e gli account istituzionali degli ex Governatori della Banca d'Italia Mario Draghi (ora Presidente della BCE) e Fabrizio Saccomanni:

Email	Date	Previous	LastSender
matteorenzi[redacted]	30/06/2016 07:08	12/06/2016 11:18	antoniaf@poste.it
mario.draghi[redacted]	09/07/2016 19:41	23/06/2016 06:06	mmarcucci@virgilio.it
fabrizio.saccomanni@[redacted]	30/06/2016 10:00	20/06/2016 06:31	l.julia@blu.it
papa' a[redacted]	24/11/2012 02:58	16/10/2012 19:46	
walter.ferrara[redacted]	09/06/2016 14:55	22/05/2016 06:01	g.simeoni@inwind.it
vincenzo.scotti[redacted]	05/07/2016 22:57	22/06/2016 06:20	d.latagliata@live.com
p.fassino[redacted]	01/07/2016 08:58	17/06/2016 06:08	rita.p@blu.it
p.bonaiuti[redacted]	02/07/2016 17:55	16/06/2016 06:30	b.gaetani@live.com
mv.brambilla[redacted]	02/07/2016 12:39	19/06/2016 06:24	gpierpaolo@tin.it
luca.sbardella[redacted]	01/07/2016 06:17	13/06/2016 06:22	e.barbara@poste.it
t.larussa[redacted]	08/07/2016 13:38	23/06/2016 06:08	stoccod@libero.it
f.cicchitto[redacted]	08/06/2016	20/05/2016	g.capezzone@virg

	05:22	06:28	ilio.it
d.capezzone[redacted]	09/06/2016 10:37	21/05/2016 06:07	baldarim@blu.it
mario.monti[redacted]	06/06/2016 15:49	20/05/2016 06:39	t.elsajuliette@blu.it
mario.monti[redacted]	30/06/2016 23:20	20/06/2016 06:05	dipriamoj@alice.it
vincenzo.fortunato[redacted]	03/07/2016 17:26	22/06/2016 06:36	giannaa@poste.it
mario.canzio[redacted]	03/07/2016 06:11	15/06/2016 06:38	izabelle.d@blu.it
poletti@[redacted]	09/06/2012 07:14	11/05/2012 16:53	
capolupo.saverio[redacted]	13/11/2012 08:00	12/10/2012 05:25	

Per un elenco più dettagliato del contenuto del database *"InfoPyramid.accdb"* si rimanda all'allegata annotazione (vds. allegato 9)

Ancora, il server avente indirizzo IP **216.176.180.181**, avente hostname *riga.westlands.com*, utilizzato come replica del server avente indirizzo IP **216.176.180.188** ha svelato ulteriori elementi utili all'indagine.

Dall'analisi del traffico SMB intercettato sull'utenza fissa in uso a Giulio OCCHIONERO, è stato possibile ricostruire la struttura delle directory sfogliate dall'utente e presenti su questo server, oltre al contenuto dei file transitati (corrispondenti ai file che l'indagato ha prelevato dal server *"riga"* e scaricato sul proprio PC).

Si descrivono di seguito le principali cartelle individuate:

1) *Hanger*: contiene i file esfiltrati dalle vittime, suddivisi in sottocartelle, ciascuna delle quali raccoglie una differente tipologia di dati, come di seguito indicato:

chrmp:	*chrome passwords*
configuration:	*configurazione della macchina infetta e folder sul PC*

emp:	*email password*
fav:	*preferiti del browser*
graph:	*collegamenti email tra le vittime*
ia:	*lista del software installato*
ieh:	*internet explorer history (cronologia di I.E.)*
iep:	*passwords salvate su internet explorer*
mozh:	*mozilla history (cronologia di Firefox)*
msnp:	*messenger passwords*
nfo:	*informazioni catturate tramite il tool msinfo32.exe*
nk2:	*cache dei nomi alternativi di outlook*
nwp:	*network passwords*
prdk:	*product id e cd-keys di software Microsoft*
recf:	*file*
shortcuts:	*link a file e directory locali o remote*
skype:	*database delle conversazioni skype*
src:	*ricerche effettuate sui motori di ricerca*
usb:	*history dei dispositivi usb connessi*
wlk:	*wireless networks passwords*

2) *MDaemon*: contiene i file di configurazione del demone[22] di posta elettronica utilizzato per la gestione dei dati carpiti dal malware, denominato *MailDemon*. Si è analizzato il file *HIWATER.MRK*, al cui interno sono state trovate informazioni relative ai nomi delle cartelle di posta presenti sul server, agli utenti ed all'oggetto dei messaggi email ricevuti.
Si evidenzia come tra i nomi delle cartelle, compaiano anche stringhe composte di 4 o 5 caratteri, che corrispondono a quelle presenti nel campo Nick del database *InfoPyramid* precedentemente descritto. Le stesse stringhe compaiono inoltre anche nel file *HIWATER.MRK* alla voce *#hostpenta.com/contacts*.
È stato poi riscontrato che l'oggetto dei messaggi email ricevuti contiene l'identificativo univoco che il malware dà a ciascuna delle vittime e che in base all'identità della vittima, questo viene memorizzato in una data locazione:

22 un demone (*daemon* in inglese) è un programma eseguito in background, cioè senza che sia sotto il controllo diretto dell'utente, tipicamente fornendo un servizio all'utente

[MailRouting]

Rule0=If <SUBJECT> contains "AS5745G Utente 00359-OEM-8992687-00006 29649A13" then move to [Global]

Rule1=If <SUBJECT> contains "MARIO-PC mario 00359-OEM-8992687-00015 DA7B17F2" then move to [Global]

Rule2=If <SUBJECT> contains "PAOLASTUDIO HP_Administrator 76434-OEM-0011903-00106 01CC31C4" then move to [Global]

Rule3=If <SUBJECT> contains "PC-ALESSANDRO Alessandro 89578-OEM-7332157-00211 44531959" then move to [Global]

Rule4=If <SUBJECT> contains "PC-DELIA Delia 89578-OEM-7332157-00204 BE4E7074" then move to [Global]

Rule5=If <SUBJECT> contains "SALAPROF Utente 55274-641-1996064-23453 4FC2F11A" then move to [Global]

Rule6=If <SUBJECT> contains "MARIO-PC MARIO 00359-OEM-8992687-00006 3E538BA7" then move to [Global]

Rule7=If <SUBJECT> contains "PC Nuova Mar jonio 00371-OEM-8992671-00521 B0CF4FED" then move to [Global]

3) *Reports*: contiene un sottocartella denominata 2016, al cui interno sono presenti numerosissimi file di testo con estensione *.txt*, che contengono i dati carpiti dal modulo di *keylogging* che il malware installa sui PC delle vittime.

L'analisi del traffico SMB ha inoltre permesso di individuare le differenti tipologie di file generati dal *malware* a seguito dell'infezione dei PC delle vittime, che sono sostanzialmente di tre tipi:

- *file xml*: contengono informazioni sottratte direttamente dalle macchine infette. Si è riscontrato che ogni vittima genera più file xml, uno per ciascuna tipologia di dati sottratti, che viene indicata da una sigla inserita nel nome del file. Tali file vengono poi memorizzati nel server C&C[25] e catalogati in differenti cartelle, a seconda del tipo di informazioni che contengono (ad es. le password per la posta elettronica, sono inserite in file xml il cui nome

[25] un *Command and Control* (C&C) è un server utilizzato per controllare l'azione di un malware (e più in generale di una botnet), inviando file di configurazione alle macchine compromesse, o raccogliendo i dati da esse carpiti.

contiene la stringa EMP, che vengono poi tutti memorizzati nella cartella EMP del server C&C).

Un esempio di come è strutturato il nome di tali file è il seguente:

INIVDCIANI a.ciani 00371-OEM-8992671-00007 2F0D873F emp.xml

dove *INIVDCIANI* corrisponde al nome del PC, *a.ciani* al nome utente, *00371-OEM-8992671-00007 2F0D873F* è l'identificativo univoco dell'utente ed *emp* indica la tipologia di informazioni contenute nel file.

Si riportano di seguito degli esempi relativi ad alcune delle tipologie dei file XML, con un estratto del loro contenuto:

FILE CHRM: <chrome_passwords_list>

<action_url>https://puntofisco.agenziaentrate.it/PuntoFiscoHome/j_security_check</action_url>

<user_name>MNTDNC51M20F839X</user_name>

<password>Castella8</password>

<action_url>https://webmail.pec.it/login.html</action_url>

<user_name>comune.concerviano@pec.it</user_name>

<password>xtIWw1QM</password>

<action_url>https://sister.agenziaentrate.gov.it/Servizi/j_security_check</action_url>

<user_name>LRSGNN82B41F158W</user_name>

<password>FIRESPA2016!!</password>

FILE EMP: <accounts>

<email>daniele.pacioni[redacted]it</email>

<display_name>Avv. Daniele Pacioni</display_name>

<account_name>Daniele Pacioni</account_name>

<pop3_server>pop3.[redacted]</pop3_server>

<pop3_user>daniele.pacioni[redacted]it</pop3_user>

<pop3_password>danielepacioni</pop3_password>

<email>danielepacioni@[redacted]</email>

<display_name>Avv. Daniele Pacioni</display_name>

<account_name>danielepacioni[redacted]</account_name>

<pop3_server>mbox.cert.legalmail.it</pop3_server>

<pop3_user>M3015452</pop3_user>

<pop3_password>27052013lucio</pop3_password>

FILE IEP: <internet_explorer_passwords_list>

<entry_name>https://owa.phc.firespa.it/</entry_name><type>AutoComplete</type><st

ored_in>Regi????</stored_in>

<user_name>silvia.galletta</user_name>

<password>SG2016!!</password>

FILE NWP <network_passwords_list>

<item><item_name>Domain:target=AVVOCATO</item_name>

<type>Domain Password</type>

<user>GIACOMO-PC\avvocato</user>

<password>gia76como$</password>

- *file gpli:* contengono elenchi di indirizzi di posta elettronica e sono verosimilmente utilizzati per delineare quali sono le persone più "vicine" alla vittima, ossia quelle con cui questi comunica maggiormente attraverso messaggi di posta elettronica.
- *file txt:* sono i file generati dall'attività di *keylogging* e, come già evidenziato, sono memorizzati nella cartella del C&C denominata *"report/2016"*. Il modo con cui vengono nominati tali file è analoga a quella illustrata per i file xml:

20160924-092052 [0] PCROMA13-1 c.ciani 00371-OEM-9044722-11968 F21C4016.txt

ove l'unica differenza con la struttura dei nomi dei file xml sta nell'indicazione di data ed ora in cui le informazioni sono state catturate.

Come già evidenziato, in questi file sono registrate le informazioni catturate dal *keylogger*, ognuna delle quali viene distinta da un "*tag*" che ne indica il tipo. Se ne riporta di seguito un breve estratto dal quale si evince come venga registrato sia ciò che viene digitato sulla tastiera (come le password o i messaggi email) che ogni azione effettuate sul PC (ad es. l'apertura o la modifica di documenti, ecc.):

[09/23/2016 | 11:12:09] [WINDOW] [TMDIForm_2]
[09/23/2016 | 11:12:09] [PROCESS] [\\Server\winfarm\WinFarm.exe]
[09/23/2016 | 11:12:09] [TITLE] [Winfarm Evoluzione Rel. 01.52.01 - FARMACIE TORNAGHI SNC - VILLA ADRIANA TIVOLI (RM) - Codice 00543]
09/23/2016 | 11:35:31] [PROCESS] [C:\Programmi\Mozilla Thunderbird\thunderbird.exe]
[09/23/2016 | 11:35:32] [WEB] [Invio copia ft 5415070021FARMACIE TORNAGHI S.N.C. cod 30131353 - Posta in arrivo - farmaciatornaghi[redacted]Mozilla Thunderbird]

.....

[09/23/2016 | 11:36:23] [EDIT] [Cerca <Ctrl+K>]
[09/23/2016 | 11:36:23] [TEXT] [Da]
[09/23/2016 | 11:36:23] [TEXT] [Da: Giannelli, Emiliano [CONIT] <egianne@ITS.JNJ.com>]
[09/23/2016 | 11:36:23] [TEXT] [Giannelli, Emiliano [CONIT] <egianne@ITS.JNJ.com>]
[09/23/2016 | 11:36:23] [TEXT] [Oggetto]
[09/23/2016 | 11:36:23] [TEXT] [Oggetto: Invio copia ft 5415070021FARMACIE TORNAGHI S.N.C. cod 30131353]
[09/23/2016 | 11:36:23] [TEXT] [A]
[09/23/2016 | 11:36:23] [TEXT] [A: farmaciatornaghi[redacted] <farmaciatornaghi@virgilio.it>]
[09/23/2016 | 11:36:23] [TEXT] [Me <farmaciatornaghi[redacted]>]

.....

[09/23/2016 | 11:36:23] [EDIT] [Buongiorno,]
[09/23/2016 | 11:36:23] [EDIT] [In allegato trova la copia della fattura da lei richiesta.]

....

[09/23/2016 | 12:15:37] [FILECHANGED] [C:\Documents and Settings\winfarm\Documenti\GIORGIO NON TOCCARE\Desktop.ini]

...

[09/23/2016 | 12:57:06] [FILECHANGED] [C:\Documents and Settings\winfarm\Documenti\Downloads\DistintePagamenti (36).pdf]

[09/24/2016 | 10:56:52] [KEYS] H3454

[09/24/2016 | 10:56:52] [WEB] [Login - Google Chrome]

[09/24/2016 | 10:56:52] [URL]

[https://ihb.cedacri.it/hb/authentication/login.seam?abi=03440&lang=it]

[09/24/2016 | 10:56:58] [KEYS] DH241599

Si riporta di seguito un elenco dei tag rilevanti generati dall'attività di keylogging:

KEYS	tasti digitati
LOGSAVED	data di salvataggio del log
FILECREATED	creazione di file
FILECHANGED	modifica di file
FILEDELETED	cancellazione di file
PROCESS	processi eseguiti
URL	URL visitate o digitate
LOGSTOPPED	data in cui è stato fermato il log del keylogger
LOGSTARTED	data in cui è iniziato il log del keylogger
HGRVERSION	versione del malware
GHKVERSION	versione del malware
ACTIVATION DATE	data di attivazione del keylogger
IPADDRESS	indirizzo IP con cui la vittima si è connessa ad internet
TEXT	testo di mail, indirizzi di posta elettronica
ORGANIZATION	nome dell'ISP utilizzato dalla vittima per l'accesso ad internet
ISP	nome dell'ISP utilizzato dalla vittima per l'accesso ad internet
GHKVERSION	versione del modulo GHK del malware (ossia il modulo di logging responsabile della registrazione delle attività dell'utente).

HGRVERSION	versione del modulo HGR del malware (ossia il modulo principale del malware, responsabile delle principali comunicazioni con l'infrastruttura C&C e del prelievo ed invio dei dati dalla macchina della vittima)

Analizzando i dati aventi *tag* [ACTIVATIONDATE] all'interno dei file txt ricostruiti a partire dal traffico telematico intercettato sull'utenza fissa in uso a Giulio OCCHIONERO, è stato possibile determinare come alcune delle vittime siano state infettate già a partire d

al mese di marzo 2014 e che l'infezione di nuove vittime sia continuata quantomeno fino all'agosto 2016:

[09/29/2016 | 18:59:30] [ACTIVATIONDATE] [Friday, March 28, 2014]

[08/19/2016 | 07:35:33] [ACTIVATIONDATE] [Wednesday, August 03, 2016]

Risulta , altresì , che sul server *riga* erano presenti numerose cartelle create negli anni precedenti (risalenti almeno al 2012), ed è pertanto ragionevole ritenere che l'attività delittuosa oggetto del procedimento fosse in essere da diversi anni.

Si evidenzia inoltre come si sia accertato che il contenuto delle cartelle *hunger* e *reports/2016* presenti sul server *riga*, precedentemente descritte nel dettaglio, fosse sincronizzato[24] con quello delle omonime cartelle presenti in locale sul PC di Giulio OCCHIONERO (avente nome host *GAMMA*), il quale pertanto riceveva regolarmente sul suo PC tutti i dati che il malware carpiva dai PC delle vittime, inviandoli poi al server di C&C.

Sono stati poi identificati numerosi collegamenti effettuati da Giulio OCCHIONERO verso il server di posta del dominio *gmx.com* che, come indicato nella relazione tecnica redatta dalla MENTAT (*cfr. pagg 57 e segg. dell'allegato 3*), corrisponde al dominio cui appartengono le caselle email utilizzate dal malware per le operazioni di *data exfiltration* dai PC delle vittime.

L'esame del traffico dati transitante sull'utenza fissa in uso a Giulio OCCHIONERO ha poi permesso di riscontrare la presenza di diverse connessioni verso i seguenti servizi di *Cloud*:

[24] La sincronizzazione del contenuto delle cartelle avveniva per mezzo del software *SyncToy*

dav.box.com

webdav.4shared.com

webdav.hidrive.strato.com

webdav1.storegate.com

che, come accertato, corrispondono agli spazi di Cloud utilizzati come C&C dal malware (*cfr. pagg. 30 e segg. dell'allegato 3*)

Dall'analisi dei file che l'indagato Giulio OCCHIONERO ha prelevato dal server "*riga*" e scaricato sul proprio PC, rilevati nel traffico di tipo *SMB* precedentemente descritto, è stato pure possibile identificare una parte delle persone o società che gli indagati hanno infettato tramite il loro malware e dai cui PC prelevavano abusivamente dati e documenti, significando che, data l'enorme mole di dati, l'analisi volta ad identificare la totalità delle vittime è tuttora in corso.

Si riporta di seguito un **elenco delle vittime più significative** dell'infezione, costituite per la maggior parte da studi legali e professionali, rimandando, per una descrizione più dettagliata delle circa 100 macchine compromesse finora identificate, all'allegata annotazione redatta dalla P.G.

STUDI LEGALI

È stata accertata la compromissione di 20 studi legali, molti dei quali specializzati in diritto amministrativo e commerciale:

- AVVOCATO MAURIZIO SCELLI

  Avvocato civilista e Parlamentare della XVI Legislatura (eletto nel PdL)

- STUDIO LEGALE GHIA (Avv. Ghia Lucio)

  Studio legale con sedi a Roma e Milano, specializzato in Diritto Societario, Commerciale, Fallimentare e Bancario.

  Risultano essere compromessi almeno 5 PC della rete dello studio, in uso all'Avv. Andrea Pivanti, alla collaboratrice Marianna Spallucci ed ai dipendenti Cristina Ciani, Elisa Millevolte (segreteria) e Giovanni Tomaso (amministrazione).

- STUDIO LEGALE BERNARDI E ASSOCIATI

  Studio legale e commerciale specializzato nel diritto commerciale, amministrativo e tributario.

  Risulta essere compromesso il PC dell'Avv. Cristina Comastri, specializzata in obbligazioni e contratti ed in diritto di famiglia.

- STUDIO LEGALE CANCRINI E PARTNERS

Studio Legale con sede a Roma, presta assistenza e consulenza legale nel campo del diritto amministrativo, del diritto civile, commerciale e societario.

Risulta essere compromesso il PC dell'Avv. Adriana Amodeo; sono inoltre stati trovati riferimenti di un secondo PC infetto, utilizzato dal Prof. Marco Macchia (professore associato di Diritto Amministrativo presso l'Università di Roma Tor Vergata)

- STUDIO LEGALE PISELLI & PARTNERS

Studio legale (con sedi a Roma, Cagliari, Mestre, Londra e Bucarest) specializzato nei servizi di consulenza, assistenza e rappresentanza ad imprese private ed Enti pubblici in contenziosi amministrativi, civili, tributario-fiscali, contabili e arbitrali, con particolare riferimento alla contrattualistica pubblica.

Risultano essere compromessi almeno 2 PC della rete dello studio, in uso agli utenti "Federica" (probabilmente in uso all'Avv. Federica Rizzo) e "P.Paluzzi".

- STUDIO LEGALE MASSAFRA (Avv. Nicola MASSAFRA)

Studio legale che offre assistenza e consulenza legale in materia di diritto Civile, Amministrativo e Penale.

- STUDIO LEGALE AVV. GIUSEPPE GRECO

L'Avv. Giuseppe Greco è Professore Straordinario di diritto amministrativo presso la Facoltà di Giurisprudenza dell'Università degli Studi di Roma "G. Marconi". È inoltre direttore di un programma di ricerca applicata in tema di concessioni demaniali marittime e Giudice Tributario di Appello per il Lazio

- STUDIO COCCONI & COCCONI

Associazione professionale di avvocati e commercialisti, con sedi a Roma e Venezia, specializzato in diritto commerciale e consulenza societaria e fiscale. Risulta essere compromesso il PC del dott. Mario Emanuele Capellini, che si occupa di consulenza bancaria e finanziaria.

- STUDIO LEGALE SILENZI & PARTNERS

Studio formato da avvocati e commercialisti esperti nel settore del business advisory e fiscalità, e che offre consulenze nei settori della finanza, del credito e delle assicurazioni, rivolte principalmente al settore delle PMI.

STUDI PROFESSIONALI

STUDIO GIANLUCA PELLEGRINO

Studio commercialista di Roma

STUDIO COMMERCIALISTI ASSOCIATI GEREMIA UMBERTO E DE DONATIS FLORIANA

Studio di commercialisti

- LUIGI DOTTORINO

Consulente del lavoro

- CFN S.R.L.

Società di consulenza commerciale e finanziaria con sede a Roma

- ARCH. PIETRO BIAVA
- ARCH. ROSANNA FERRAIRONI

SOCIETÀ DI RECUPERO CREDITI

- FIRE S.p.A.

Risultano essere compromessi decine di PC della rete interna della società FIRE S.p.A.

- ESSEBI GROUP S.r.L.

società controllata dalla FIRE S.p.A.

ENTI ISTITUZIONALI

- SECONDA UNIVERSITÀ DI NAPOLI

Risulterebbe essere compromesso un PC della segreteria della Facoltà di Lettere

- REGIONE LAZIO

Risulterebbe essere compromesso il PC in uso all'Avv. Elena Prezioso, Dirigente dell'ufficio Contenzioso dell'Avvocatura Regionale

- SINDACATO CGIL FUNZIONE PUBBLICA DI TORINO

VATICANO

CARDINALE GIANFRANCO RAVASI

Risultano essere compromessi i PC in uso a due collaboratori del Card. Ravasi, dal 2007 Presidente del Pontificio Consiglio della Cultura, della Pontificia Commissione di Archeologia Sacra e del Consiglio di Coordinamento fra Accademie Pontificie.

CASA BONUS PASTOR

struttura alberghiera di proprietà del Vicariato di Roma

SOCIETA' DI COSTRUZIONI

PULCINI GROUP

Società di costruzioni fondata da Antonio Pulcini.

Risultano essere compromessi almeno due PC in uso a dipendenti della società, tra cui quello del titolare Antonio Pulcini.

COSTRUZIONI EDILI BERGAMELLI S.p.A.

Società di costruzioni con sede in provincia di Bergamo, ma che opera su tutto il territorio nazionale.

FINCHAMP GROUP

Gruppo cui fanno parte una società di costruzioni ed una immobiliare.

SANITÀ

GRUPPO INI S.p.A.

Il gruppo INI, Istituto Neurotraumatologico Italiano, presente in molte aree del Paese, conta di diverse strutture sanitarie abilitate al ricovero ed all'assistenza specialistica ambulatoriale, con circa 1.000 posti letto e oltre 1.200 dipendenti.

MUTUA MBA

Mutua MBA è la più grande mutua sanitaria italiana per numero di soci. Offre agli aderenti prestazioni mediche a costi agevolati.

COOPSALUTE S.C.p.A.

È una Società Cooperativa per Azioni nata per costituire un unico punto di incontro tra la domanda e l'offerta di prestazioni e servizi socio-sanitari ed assistenziali su tutto il territorio nazionale.

Risultano essere compromessi almeno cinque PC in uso a dipendenti della cooperativa.

ALTRO

REALE MUTUA ASSICURAZIONI

Risultano essere compromessi almeno due PC dell'agenzia 676 di Roma, e tre dell'agenzia 679.

TOTI TRANS SRL

Società di trasporti nazionali ed internazionali della provincia di Frosinone, recentemente fallita, ma i cui 150 dipendenti sono stati assorbiti dalla SLI di Frosinone

Risultano essere compromessi quasi 20 PC in uso a dipendenti della società.

L'elenco citato è stato ricavato analizzando il contenuto dei file che Giulio OCCHIONERO ha scaricato sul proprio PC nel periodo in cui la sua utenza fissa era oggetto di intercettazione telematica (ossia per poco più di un mese, a partire dal 23.08.2016) e contiene pertanto le sole vittime per le quali, nel periodo indicato, questi aveva impostato la sincronizzazione dei dati tra il server *riga* ed il PC *GAMMA* (ossia quello che utilizzava presso la sua abitazione).

Si evidenzia poi come dall'analisi dei dati ottenuti nel corso dell'intercettazione telematica attiva sia emerso che sul server *riga* erano presenti numerose cartelle create negli anni precedenti (sino all'anno 2010), e tale circostanza fa ritenere che le vittime sopra elencate siano solamente una parte del totale, costituita da quelle di interesse per gli indagati nel periodo dell'intercettazione, e che nel corso degli anni questi abbiano infettato molte altre persone e società.

Ulteriori elementi di rilievo a carico di Giulio OCCHIONERO sono emersi dall'intercettazione telematica attiva effettuata, dal 1 al 4 ottobre 2016, sul PC connesso alla linea fissa installata presso la sua abitazione (avente nome host *GAMMA*).

Si riporta di seguito un estratto degli screenshot elementi maggiormente significativi realizzati dall'agent istallato a tal scopo sul PC *GAMMA* rimandando, per una più dettagliata descrizione di

quanto emerso, alle annotazioni redatte dalla P.G. (vds. allegati 11 (attività del 1.10.2016), 12 (attività del 2 e del 3.10.2016), 13 e 14 (attività del 4.10.2016))

alle ore 11:31 del 01.10.2016 viene aperto il client di posta elettronica *"Outlook"* all'interno del quale sono presenti le seguenti cartelle: *"mail.emasrl.com"*, *"mail.me.com"*, *"mail.pulcinigroup.it"*, *"mail.register.it"*, *"pierluigi@[redacted]"*, *"mail.sergioscibetta.it"*. Nello specifico viene aperta sul client la sottocartella *"Inbox"* di *"pierluigi@[redacted]"* (ossia quella relativa alla *posta in arrivo*), e vengono consultati i messaggi in essa presenti, indirizzati a Pierluigi Mancuso.

Si evidenzia che l'account *pierluigi@[redacted]* è risultato essere presente nel database *InfoPyramid.accdb* descritto in precedenza, e che la società *PULCINI GROUP* è risultata essere una delle vittime dell'infezione da parte del malware diffuso dagli indagati.

alle ore 13:36 del 01.10.2016 nel client di posta elettronica *"Outlook"* viene visualizzata la cartella *"Inbox – Hanger"* al cui interno sono presenti numerosi messaggi email indirizzari a caselle del dominio *gmx.com*[25] (compresi sei nuovi messaggi non ancora letti indirizzati all'account di posta elettronica *ulpi715@gmx.com*) contenenti in allegato quelli che con ogni probabilità sono i file catturati dal malware (è infatti visibile il loro nome, che ha struttura uguale a quella descritta in precedenza per i file *xml* e *txt*: *"CERTKILL_ZIR3478 sara.marchesan 00371-OEM-9309501-23878.1FD4E1A0"*) e che poi, come illustrato, verranno memorizzati nella cartella *Hanger* del C&C.

alle ore 17:55 del 01.10.2016 sono stati copiati copiati 17 file da una cartella locale denominata *web* verso una cartella di rete avente percorso *\\estlands.com\Web\Sites\hostpenta.com*, chiaro indice questo di come Giulio OCCHIONERO abbia la gestione del sito *hostpenta.com*, che è risultato essere il dominio utilizzato dal malware verso cui viene replicato il contenuto delle caselle email *@gmx.com* utilizzate per le operazioni di data exfiltration.

alle ore 23.12 del 01.10.2016 viene visualizzata tramite il client di posta elettronica *"Outlook"*, anche la cartella *"Inbox – Reports"* (ossia l'altra destinazione, insieme ad *Hanger*, utilizzata dal malware per memorizzare i dati esfiltrati), e nello specifico viene visualizzato il messaggio email inviato all'indirizzo email *"ekehuj2804@gmx.com"*, avente oggetto *"[0]*

---

25 Come già descritto in precedenza, il malware esfiltra i dati dai PC delle vittime inviandoli su caselle del dominio *gmx.com*

PATRIZIA-7 Patrizia 00330-80000-00000-AA227 955E2825" ricevuta il 21.09.2016 alle ore 8:35 am, contenente in allegato l'omonimo file *txt* contenente i dati carpiti dal modulo di *keylogging* del malware.

alle ore 01:00:18 del 02.10.2016, il sistema ideato da Giulio OCCHIONERO, ha terminato le operazioni di sincronizzazione, effettuata tramite il citato software *SyncToy*, tra la cartella remota *\\westland.com\Mail\Hanger* (ove sono memorizzati i file carpiti dal malware) e quella locale *D:\Work\EyePyramid\Hanger*. Dallo screenshot si evince come le cartelle abbiano esattamente lo stesso contenuto, ossia 345120 file (per una dimensione totale di circa 87 Gbyte).

alle ore 21:22:43 del 02.10.2016, utilizza l'applicativo *Eye Manager* per la compilazione in Visual Studio del codice del malware. Nello specifico apre i moduli *Hangeron* e *Mailfaker* *(per la cui descrizione si rimanda alle pagg. 23 e segg. dell'allegato* 3) e modifica alcuni valori inerenti i certificati all'interno della classe denominata *fHangeron.Menu.Web.vb*.

Ciò è un chiaro indice di come sia proprio Giulio OCCHIONERO la persona che ha scritto il codice del malware e che ne sta curando l'evoluzione, con la costante introduzione di nuove funzionalità. *(cfr. allegato* 8)

poco dopo confronta due certificati rilasciati da Microsoft, uno presente sul pc da lui utilizzato e l'altro recuperato dal server SQL installato sul suo server remoto avente hostname *Moscow* (con IP 216.176.180.180. **Alle ore 21:56, appurato che i due certificati sono identici, invia una email alla sorella Francesca, all'indirizzo *focchionero@westlands.com*, nella quale la informa del risultato delle sue verifiche.**

Nello specifico dal testo del messaggio, in cui Giulio dice testualmente alla sorella *"Ad ogni modo è valido pure sui server (Moscow) americani quindi dubito che abbiano dato ad un'autorità italiana il privilegio di infettare macchine americane"* (*cfr. pag. 7 dell'allegato* 12), emerge chiaramente che Giulio e Francesca Maria Occhionero sono preoccupati di poter essere monitorati dalle autorità italiane[36].

Il fatto che Giulio condivida immediatamente con la sorella questi suoi timori, benché a suo carico non sia in essere alcun procedimento, e che i due parlino esplicitamente dei server appartenenti

[36] Si fa presente che, come emerso dall'intercettazione telefonica sulle utenze in uso agli indagati, in data 09.09.2016 Giulio Occhionero è venuto a conoscenza dell'instaurazione del presente procedimento penale a suo carico.

alla rete di gestione del malware, è un chiaro indice di come anche Francesca Maria OCCHIONERO sia pienamente responsabile delle condotte delittuose per cui si procede.

A tal riguardo assumono grande rilevanza dapprima l'email di risposta inviata da Francesca a Giulio qualche minuto dopo:

"Bravo! Possiamo tranquillizzarci (un po') Notte",

e poi il messaggio *WhatsApp* della mattina seguente (alle 8:25) nel quale Francesca dice testualmente a Giulio:

"Giulio ti prego di non coinvolgere mamma nei nostri problemi, mi sembra che sia già abbastanza coinvolta e che ci sta aiutando più del dovuto. Primo non dobbiamo aggiungere altri problemi, è stanca e ha bisogno di riposare e stanotte non ha chiuso occhio, secondo non può darci alcun aiuto su queste materie e terzo perché come vedi a volte sono dei falsi allarmi. ..."

Frasi, queste pronunciate da Francesca Maria Occhionero, che lasciano capire chiaramente come i due si confrontassero circa le scelte da intraprendere ed eventuali accortezze da tenere, inequivocabilmente fondando un chiaro concorso di persone nelle condotte descritte.

- alle ore 09:13:01 del 02.10.2016, viene nuovamente visualizzata, per mezzo del client di posta elettronica Outlook, la cartella *Inbox-Hanger*, contenente numerosi messaggi email indirizzati a caselle del dominio *gmx.com* tramite le quali gli indagati esfiltrano i dati dai PC delle vittime.

  Si evidenzia come tale operazione venga effettuata più volte nell'arco della giornata (si ripete alle ore 16:16:52), indice di come Giulio Occhionero controlli costantemente la presenza di nuovi dati carpiti dalle vittime.

  Dall'analisi effettuata sui dati acquisti, è stato possibile accertare che tutti i collegamenti verso i server remoti sono stati effettuati mediante l'uso dell'applicativo *remote desktop*, con autentificazione tramite smartcard e pin *112358*.

L'analisi di tali *screenshot* ha inoltre permesso di accertare come, a partire dalle ore 14.41 del 04.10.2016, Giulio OCCHIONERO abbia dato inizio alla distruzione degli elementi di prova a suo carico, cancellando dati che erano presenti sia sul suo PC locale che su alcuni dei server remoti, come meglio di seguito specificato, significando che per una dettagliata descrizione delle azioni effettuate si rimanda all'annotazione riportata in allegato 14:

- a partire dalle ore 14:42:16 ha eliminato alcune delle credenziali di accesso presenti nel suo *enallet*, ossia nel gestore di password da lui utilizzato.

- alle ore 14:56:36 ha cancellato alcuni account di posta elettronica presenti sul suo PC in locale (tra cui *Archive, Hanger* e *Reports*), eliminando i files *Archive.pst, Hanger.pst* e *Reports.pst* che contenevano tutti i messaggi di posta dei relativi account (dall'immagine si vede che tutti e tre i file in questione risultano essere stati creati il 10.02.2012).

  Si evidenzia che, come descritto in precedenza, nelle cartelle *Hanger* e *Reports* vengono memorizzati i messaggi email inviati alle caselle *@gmx.com*, tramite i quali il malware esfiltra i dati dal PC delle vittime. Eliminando i file *.pst* sopra indicati quindi, Giulio OCCHIONERO ha quindi cancellato la copia dei dati esfiltrati dalle vittime che aveva memorizzato sul suo PC.

- alle ore 15:11:43, cancella i dati esfiltrati anche dal server remoto *riga*.

A tal scopo infatti, tramite l'applicativo *Remote Desktop* di Windows, si collega al server *riga* e procede alla rimozione di tutti gli account (ad eccezione dell'account *test*) del demone di posta elettronica utilizzato per la gestione dei dati carpiti dal malware (*MailDemon*). Si elencano di seguito gli account che sono stati cancellati: *deliver3, deliver2, particular3, particular2, particular, special5, special4, special3, special2, special, deliver, gpool, hpool, index, hgr, archive, freports* e *reports*.

Successivamente, per garantirsi la totale cancellazione dei messaggi, entra all'interno della cartella *C:\MDaemon\Users\hostpenta.com* ed elimina la sottocartelle *archive* e *hpool*.

- alle ore 15:41, tramite il compilatore Microsoft Visual Studio, accede al codice del malware ed apre la classe denominata *m.Core.vb*. Dai moduli presenti, preleva le credenziali di accesso al servizio di cloud *hidrive.strato.com* e, utilizzando una connessione anonimizzata per mezzo di *torbrowser*, procede alla cancellazione degli account:
  - *veplo60822 (con password* [redacted]
  - *xema11757 (con password* [redacted]

  si evidenzia che tali account contenevano parti (nello specifico la zona denominata *Basel* dell'architettura del C&C utilizzato per la gestione del malware (*cfr. pagg. 30 e segg. dell'allegato 3*)

  Successivamente procede alla cancellazione di altri account e stringhe presenti all'interno della stessa classe, e connessi alla medesima architettura del C&C, come di seguito elencato:
  - *https://webdav.hidrive.strato.com/users/japatoa65731*
  - *https://webdav.hidrive.strato.com/users/gola34757*
  - *anulcia@msn.com*

- rimuove i valori relativi alle variabili *hgrghk, tmpwebshell e carrier*
- *https://webdav.hidrive.strato.com/users/druza29461*
- *babe1964@hotmail.it*
- *atccorp.in@gmail.com*
- *https://www.dropbox.com/s/6c579v98lmjd2o3/XIIJe8MUmvT34?dl=1*
- *https://webdav.hidrive.strato.com/wget/8DWrt2Kg*
- *MN600-849590C695DFD9BF69481597241E-668C* (licenza MailBee)
- *MN600-481597241E8D9BF6949590C695DF-774D* (licenza MailBee)
- password [redacted] presente nel modulo *PCMDPWD*
- password [redacted] presente nel modulo *WEBDECCERTPWDNEW*

- alle ore 15:57:25 accede alla classe *cEmailJob.vb* e procede alla cancellazione delle righe contenenti le variabili *ds1, ms1, dc1, ds2,ms2* e *dc2*
- alle ore 15:59:16 ritorna sulla classe *inCore.vb* e procede alla cancellazione di altre due licenze MailBee presenti nel codice:

MN600-3E3A3C593AD5BAF50F55A4ED60E0-385D

MN600-AD5BAF50F56A60E043E3A3C593ED-874A

- alle ore 16:00:17 modifica la classe *inWakeUP.vb* eliminando le seguenti credenziali:
  - *username lu_1974@hotmail.com*
  - *URL https://storage.driveonweb.de/probdav username balu9487*
  - *URL https://dav.box.com/dav username guia.gennarini@yahoo.it*
  - *URL https://webdav.cloudme.com/fugik12239/xios username fugik12239*
  - *cozzolinofrancesca[redacted]*
  - *URL https://dav.box.com/dav username ultu40166@yhaoo.co.uk*
  - *URL https://dav.box.com/dav username cucciola87ps@hotmail.it*
  - *URL http://webdav.4shared.com username eyiri33730@yahoo.es*
  - *username whatsupevents@hotmail.it*
  - *username wuldeh2207@gmail.com*
  - *username muscia_msn@hotmail.it*
  - *URL http://webdav.cloudme.com/gako6649/xios username gako6649*

- *url https://storage.driveonweb.de/probdao username luther5498*
- *username ale_pala84@hotmail.it*

- Alle ore 16:09:47, elimina alcune ricerche avanzate che aveva preimpostato sul suo PC, come di seguito elencate:
  - *(foldermessages) AND fiorillo*
  - *(folderreports) AND (vitalino,fiorillo)*
  - *(folderreports) AND (giulio,occhionero)*
  - *(folderreports) AND (postepay)*
  - *(folderreports) AND (antonio,pulcini)*
  - *(folderhanger) AND (antonio,pulcini)*
  - *(foldermessage) AND (stefano,galiardi)*
  - *(folderreports) AND gdf.it*
  - *(folderreports) AND (giuseppe,campanelli)*
  - *(folderhanger) AND (giuseppe,campanelli)*
  - *(foldermessages) AND (studiodangelo@hotmail.)*
  - *(foldermessages) AND 4shared*
  - *(foldermessages) AND theboxteam@box.com*
  - *(foldermessages) AND hidrive*
  - *(foldermessages) AND box.com*

Non è nota la sintassi esatta di tali query, ma considerandone il nome, si può ragionevolmente affermare siano riconducibili a ricerche di parole chiave effettuate in specifiche cartelle:

in tal senso, ad esempio, le query *"(folderreports) AND (antonio,pulcini)"* e *"(folderhanger) AND (antonio,pulcini)"* starebbero ad indicare due distinte ricerche delle keyword *antonio* e *pulcini* effettuate all'interno delle cartella *reports* ed *hanger* (si fa presente a tal proposito che le cartella Reports ed Hanger vengono utilizzate dal malware per memorizzare i dati esfiltrati, e che Antonio Pulcini è una delle vittime accertate di infezione).

Appare quindi evidente come le ricerche sopra elencate venissero ripetute con frequenza e da ciò sarebbe derivata l'esigenza di salvarne il contenuto per non doverlo digitare per intero ogni volta.

- Terminata tale operazione, accede alla cartella del disco locale dove è memorizzato il malware (che come noto è denominato *Eyepyramid*) e cancella alcuni file e cartelle.
  Nello specifico, alle ore 16:10:27 accede alla cartella *D:\Work\Eyepyramid\Forms* all'interno della quale sono presenti 5 sottocartelle denominate: *aol.com, email.it, gmx.com, hidrive.com* e *storagate.com* e cancella il contenuto delle cartelle *storagate.com* e *gmx.com*.
- subito dopo, alle ore 16:12:47, accede alla cartella del modulo *Mailfaker*[27] (al percorso *D:\Work\EyePyramid\Mailfaker*) ed esegue le seguenti operazioni:
  - cancella i file: *smtps.xml, graph.bak* e *tasks.xml*
  - cancella il contenuto del file alerts.txt
- alle ore 16:14:41 cancella anche la cartella *D:\Work\EyePyramid\Networking*.
- alle ore 16.15.19 accede alla cartella D:\Work\EyePyramid\Obj e, utilizzando un editor XML (XML Notepad) modifica i file *params.xml, wuc.xml* e *jfbc.xml*
- alle ore 16:16:06 cancella la cartella D:\Work\EyePyramid\Reference), che contiene quelli che paiono essere file *doc* e *pdf* esfiltrati dai PC delle vittime e che hanno date di ultima modifica comprese tra il 29.10.2010 ed il 05.05.2011.

Quanto ricavato dalle intercettazioni telematiche può essere completato dai rilevanti elementi emersi anche dalle attività di **intercettazione telefonica**, con particolare riferimento a quella effettuata sull'utenza mobile 347/2384800 intestata ed in uso a Giulio OCCHIONERO, come di seguito riportato nel dettaglio. **(vds. allegato 15)**

- alle ore 10:41:19 del giorno 31.07.2016, Giulio OCCHIONERO parla con la sorella Francesca Maria ed inizialmente i due discutono di una proposta di lavoro che lui avrebbe ricevuto e per la quale avrebbe dovuto trasferirsi a Berlino per 5 mesi.
  Giulio poi parla alla sorella dei corsi di informatica che sta seguendo, tra cui uno su SQL Server[28], a proposito del quale le dice: *"...l'ho usato un po', ma lo sto usando me lo so installato e tra l'altro ci sto deviando certi log dei nostri così..."*.
  Tale affermazione, palesemente riferita ai log dei server facenti parte l'infrastruttura di gestione del malware (descritti nel dettaglio in precedenza), nella quale Giulio parla al

27 Il modulo Mailfaker ha il compito di inviare messaggi email "contraffatti" come mezzo di propagazione del malware (cfr. pag. 25 dell'allegato 3)

28 SQL Server è un sistema relazionale di gestione di database prodotto dalla Microsoft.

plurale, lascia chiaramente intendere come siano entrambi partecipi nelle condotte delittuose di cui al presente procedimento.

La partecipazione di Francesca Maria Occhionero appare, poi, ulteriormente confermata dalla conversazione avvenuta tra i due fratelli alle ore 17:17:24 del giorno 08.08.2016, quando lui le dice: *"...Se ti serve un SQL replicato lì, a parte che noi ce li abbiamo i server, ma te lo metti lì, guarda c'è gente che vive avendo creato un app per far due stronzate..."*. Si evidenzia infatti come, parlando dell'infrastruttura in questione, continui ad usare il plurale, ad indicare come questa sia gestita da entrambi.

Rilevanti elementi circa le responsabilità di Francesca Maria OCCHIONERO sono infine emersi anche dalle attività di intercettazione telefonica sull'utenza mobile [redacted] lei intestata, come di seguito riportato nel dettaglio. **(vds. allegato 17)**

Alle ore 12.01.30 del giorno 05.10.2016 infatti, l'indagata riceve una chiamata da parte di un tecnico del suo Internet Service Provider (*la società McLink*), che le chiede se è stato risolto il problema che questa aveva lamentato. Lei risponde che ha ancora problemi ad accedere tramite la sua linea fissa alle cartelle condivise che ha sul dominio *westlands.com*, mentre riesce ad accedervi regolarmente utilizzando la connessione del cellulare. Francesca Maria Occhionero poi aggiunge: *"...Per me è fondamentale perché sono directory condivise di un dominio Microsoft di lavoro, quindi...io lavoro da remoto, quindi io devo poter accedere a quelle cartelle..." "...dunque, io per accedere che cosa faccio, io apro esplora risorse e chiamo slash slash ed il dominio, che è westlands.com, a quel punto lui di solito, mi faceva sfogliare tutte le cartelle condivise, di questo dominio westlands, adesso invece mi nega l'accesso, dice non è possibile raggiungerlo..." "...il dominio è fuori a Chicago, in America..." "...non ha le credenziali perché noi accediamo con smartcard..."*

Dal contenuto della telefonata appare evidente quindi come anche Francesca Maria OCCHIONERO sia solita connettersi ai server del dominio *westlands.com*, che come è stato accertato corrispondono ai server di C&C del malware e sfogliare le cartelle accedendo ai file in esse contenuti, ossia ai dati esfiltrati dalle vittime.

A ulteriore completamente del presente compendio probatorio e per meglio definire le responsabilità di entrambi gli indagati per i fatti per cui si procede, giova evidenziare quale sia stato l'atteggiamento tenuto da Giulio e Francesca Maria OCCHIONERO nel corso delle perquisizioni domiciliari cui sono stati oggetto in data 05.10.2016.

I due, resosi conto della presenza degli operanti innanzi alla porta della propria abitazione grazie ad un complesso sistema di videosorveglianza, hanno così agito:

- Giulio OCCHIONERO è immediatamente tornato nella stanza adibita a studio ed ha riavviato il suo PC (che evidentemente era regolarmente acceso) sul quale era installato il sistema di cifratura BitLocker della Microsoft, rendendo in tal modo impossibile l'accesso ai dati in esso contenuti;
- Francesca Maria OCCHIONERO, nel corso della perquisizione effettuata nell'abitazione della madre ove era stato rinvenuto un PC acceso e bloccato sulla schermata di login, alla richiesta di fornire la password di accesso l'indagata ha digitato più volte una password errata, causando il blocco definitivo della smart card.

Non solo, ma durante la successiva perquisizione effettuata presso la sua abitazione Francesca Maria OCCHIONERO, nell'atto di assistere alle attività, ha compiuto un gesto repentino lanciandosi verso un PC portatile che era acceso e, dopo aver inutilmente tentato di impartire comandi dalla tastiera, riusciva a sfiorare la smart card in esso inserita, sfilandola leggermente dalla sua sede e causando il blocco del sistema operativo.

In altre parole, entrambi gli indagati hanno posto in essere comportamenti manifestamente e univocamente indicativi della loro volontà di impedire l'accesso alle memorie dei propri personal computer, al fine di evitare il rinvenimento di elementi probatori rilevanti per il procedimento penale *de quo*.

Qualificazione giuridica dei fatti

Chiaramente integrati risultano i reati in epigrafe indicati, tutti evidentemente compiuti all'interno di un medesimo disegno criminoso volto ad acquisire, mediante l'utilizzo di malware, informazioni e dati sensibili che permettessero ai due di avvantaggiarsi nel mondo della politica e dell'alta finanza, grazie a un cospicuo patrimonio conoscitivo nelle disponibilità dei professionisti che vi operano e delle autorità pubbliche di riferimento.

La costante attività di monitoraggio delle comunicazioni, così come posta in essere dai due indagati, ha integrato la violazione di più norme incriminatrici:

In primo luogo è configurabile il delitto di accesso abusivo a sistema informatici/telematico (art. 615 ter c.p.); condotta che ricorre in tutte le occasioni nelle quali il sistema informatico bersaglio della condotta di hackeraggio sia stato infettato utilizzando il malewere EyePiramid. Infatti il predetto virus consente l'accesso indiscriminato, da remoto, ai sistemi infettati e, quindi, li sottopone ad attività di controllo a distanza realizzata sia attraverso l'imposizione di comandi da parte dell'hacker, sia attraverso estrapolazione generalizzata o mirata dei suoi contenuti. La protezione informatica, di cui i sistemi infiltrati sono muniti, viene sistematicamente violata sia al momento dell'accesso iniziale per l'inoculazione del virus, sia nei momenti successivi nei quali l'hacker accede al sistema infettato per imporgli ordini a distanza o per captare i contenuti ivi custoditi. In sostanza, ogni condotta di infezione di un sistema comporta un numero indeterminabile di accessi abusivi successivi, conseguenza imprescindibile dell'azione di infezione informatica. Peraltro il virus utilizzato possiede anche la funzione di keylogger e quindi carpisce e trasmette al centro di Comando & Controllo tutte le chiavi di accesso informatico conservate nel sistema o utilizzate dal suo titolare nel corso di connessioni web. Conseguentemente mette in condizione l'hacker di accedere abusivamente a tutti gli account in possesso del titolare del sistema infettato (caselle di posta elettronica, cluod, conti correnti on line, profili social ecc.). La fattispecie contestata assume, inoltre, la forma aggravata prevista dall'ultimo comma dell'art. 615 ter c.p. attesa la natura di molti dei sistemi infettati, atteso che in molti casi i sistemi informatici aggrediti sono certamente di interesse militare o relativi all'ordine e sicurezza pubblica o, comunque, di interesse pubblico. Sussiste, in fine l'ulteriore aggravante di cui al comma 2° n. 3 dell'art. 615 ter c.p., atteso che la natura del virus inoculato certamente altera il funzionamento del sistema infiltrato interrompendone parzialmente le funzionalità originarie, prime tra tutte quelle di protezione, predisposte proprio al fine di preservarlo da interferenze esterne. Non si può trascurare, sul punto, che ogni malware, oltre a permettere l'esportazione dei dati, comporta la modificazione\alterazione del sistema informatico infiltrato, alterandone il funzionamento con grave rischio per la sicurezza delle operazioni gestite dal sistema informatico. Tale ulteriore pericolo appare

estremamente grave quando i servizi resi dal sistema informatico violato pertengono alla sicurezza nazionale. Basti pensare al primo atto scoperto, grazie al quale si è potuti risalire alle condotte illecite descritte: il tentativo di hackeraggio del sistema informatico dell'ENAV, contenente informazioni e dati relativi alla sicurezza pubblica nel settore dell'aviazione civile.

Inutile spiegare quanto delicate – e cruciali per la sicurezza nazionale - siano informazioni relative all'ente nazionale aviazione, alle rotte di volo, ai dati dei dipendenti, ove soprattutto si consideri il clima politico mondiale odierno.

La pena edittale per le condotte sussumibili all'art. 615 ter c.p. è da uno a cinque anni di reclusione per l' ipotesi aggravata di cui al co. 2 n. 3 del citato articolo aumentata nel caso in cui il sistema informatico infettato rivesta interesse pubblico nei termini indicati dal comma 3 della medesima norma da tre ad otto anni il che rende , quindi , applicabile la richiesta misura della custodia cautelare in carcere .

Le fattispecie di cui agli artt. 617 quater e 617 quinquies c.p., entrambe nella forma aggravata, ricorrono, invece, in relazione alle condotte di installazione abusiva, nei sistemi informatici hackerati, di softwere idonei ad intercettare comunicazioni telematiche e nella conseguente attività di intercettazione abusiva del traffico telematico generato dai sistemi infettati. La finalità di interesse pubblico alla quale sono serventi molti tra i sistemi informatici infettati determina la configurabilità delle circostanze aggravanti di cui all'art. 617 quater co. 4° n. 1) e 617 quinquies comma 2° che, con effetto speciale, fissano le rispettive pene edittali da 1 a 5 anni di reclusione.

Sul particolare disvalore dei fatti narrati, in ultimo, si sottolinea che l'ulteriore acquisizione dei contenuti (dati, informaziopni ed atti) già sottratti dagli indagati e conservati attualmente su server esteri oggetto di attività rogatoriali già avviate, apre ulteriori spazi per l'aggravamento delle contestazioni, atteso che, una volta dimostrata la segretezza di alcuni di essi e la loro pertinenza al settotre politico e /o militare, già oggi altamente probabile, sarebbe inevitabile qualificare ricondurre le azioni criminose nell'ambito die delitti contro la personalità dello Stato (artt. 256 e 257 c.p.) .

ESIGENZE CAUTELARI

L'analisi dei singoli episodi ricostruiti nel presente procedimento mostra chiaramente che non si tratta di condotte isolate ma di un *modus operandi* dei due indagati che, per anni, hanno gestito i loro affari e interessi economici e personali secondo le descritte modalità illecite.

Oltretutto, il ricorrere di alcuni indizi probatori anche in altri procedimenti aventi similare oggetto lascia intendere che la presente vicenda non sia un' isolata iniziativa dei due fratelli ma che, al contrario, si collochi in un più ampio contesto dove più soggetti operano nel settore della politica e della finanza secondo le modalità sin qui descritte.

Ci si riferisce, in particolare al diretto collegamento tra le condotte oggetto di imputazione ed interessi illeciti oscuri desumibile dal rinvenimento, nel corso delle indagini di 4 caselle di posta elettronica già utilizzate per attività similari, secondo quanto emerso dalle indagini relative alla c.d. P4, aventi ad oggetto, anch'esse, *«l'illecita acquisizione di notizie e di informazioni, anche coperte da segreto, alcune delle quali inerenti a procedimenti penali in corso nonché di altri dati sensibili o personali al fine di consentire a soggetti inquisiti di eludere le indagini giudiziarie ovvero per ottenere favori o altre utilità».*

Ciò premesso , ed al di là di qualsivoglia collegamento , allo stato non dimostrato con altri procedimenti penali , non può dubitarsi della sussistenza di un concreto e attuale pericolo che Giulio e Francesca Maria OCCHIONERO, qualora permangano in libertà, commettano altri delitti della stessa specie di quelli per cui si procede.

Primo dato da cui desumere tale concreto pericolo è costituito dalla riscontrata protrazione di tale illecita attività per un lunghissimo periodo(sin dagli anni 2011-2012) il che è coerente con gli ingenti quantitativi di dati raccolti, le numerose persone seguite, i

consistenti numeri dei soggetti istituzionali e dei sistemi informatici di interesse pubblico monitorati mediante il *malware*.

La ripetitività e la pervicacia delle condotte delittuose si accompagnano , peraltro , alla grande spregiudicatezza con la quale i due indagati le hanno poste in essere di cui appare manifestazione anche il comportamento dai medesimi tenuto volto ad impedire l' accertamento delle medesime mediante una attività , come si è illustrato , chiaramente preordinata ad inquinare il quadro probatorio , attraverso una sistematica distruzione delle prove .

Al riguardo lo stesso atteggiamento dai due fratelli Occhionero tenuto in occasione delle perquisizioni coridotte dalla P.G. presso i rispettivi domicilii appare connotato , come si preciserà in seguito , da una notevole scaltrezza dalla quale pure è dato desumere una abitualità delle illecite condotte ed un assoluta inconsapevolezza del disvalore delle stesse.

Orbene , in tale contesto il pericolo di recidivanza è più che concreto ed attuale e l' intensità dello stesso rende assolutamente necessario il ricorso alla misura custodiale che appare l' unica in grado di escludere la reiterazione di reati della stessa indole , limitando in maniera assoluta la possibilità di utilizzo di qualsivoglia strumento tecnico a ciò necessario .

Non può , infatti , non essere evidenziato come sia sufficiente una dotazione informatica minima (costituita da uno smartphone e una connessione internet) per continuare a monitorare l'operatività dei malawere già attivati , il che rende del tutto inadeguato il ricorso alla misura cautelare degli arresti domiciliari o a misure meramente prescrittive , pure applicate cumulativamente , stante l' assenza di alcun significativo effetto deterrente non precludendo queste la possibilità di perseverare nei comportamenti contestati .

Non solo, come già detto ,la reiterazione delle condotte appare assai agevole sottro il profilo tecnico , ma pure va evidenziato come - essendo l'intera struttura di controllo della *botnet*, tramite la quale si è accertato che gli imputati gestiscono i P.C. compromessi, ospitata su server internet ubicati all'estero – non è possibile procedere al loro sequestro il

che non consente di frapporre alcun ostacolo agli indagati al loro utilizzo, per un determinato periodo, al fine di trasferire altrove il controllo della botnet e salvare l'ingente contenuto di dati ed informazioni sino ad ora illecitamente acquisito.

Tale circostanza, peraltro permette ai prevenuti di poter cancellare le prove a loro carico, evidenziando la concorrenza dell'ulteriore esigenza cautelare del **pericolo di inquinamento probatorio**, che appare concreta e non astrattamente prevedibile in ragione della condotta di occultamento e distruzione delle prove già consumata da entrambi gli Occhionero.

Si sottolinea, infatti, come sia emerso dall' attività investigativa svolta come alcuni dati informatici, fonte di ulteriore riscontro delle condotte illecite commesse, siano stati già cancellati dai predetti quando questi hanno cominciato a sospettare dell'esistenza del presente procedimento.

Tale attività di cancellazione non ha tuttavia riguardato la maggior parte dei dati già immagazzinati su server collocati all'estero, la cui acquisizione è oggetto di procedura di rogatoria già avviata presso l'autorità giudiziaria statunitense.

Tentativi di accedere nuovamente a tale infrastruttura e al controllo della *botnet* sono peraltro già emersi quando, in data 08.10.2016, come descritto in precedenza, Giulio Occhionero richiedeva ed otteneva un codice di accesso per il dominio della *Westlands Securities*, presumibilmente allo scopo di autenticarsi anche in assenza delle *smart card* utilizzate in precedenza, e poste sotto sequestro in data 05.10.2016.

La volontà degli indagati di distruggere ogni fonte di prova si palesava chiaramente già in data 04.10.2016, quando Giulio OCCHIONERO eliminava sia i dati abusivamente carpiti dai PC vittima di infezione, che il codice stesso del virus da lui sviluppato, cancellando inoltre alcuni account di servizi di *Cloud Storage* che erano nella sua disponibilità e che contenevano elementi rilevanti per il procedimento per cui si procede. (*cfr allegato 14*)

Ad ulteriore riprova di tale volontà, si riferisce come i competenti uffici dell'FBI statunitense di Washington e Seattle, cui l' Ufficio del P.M. si era rivolto per il congelamento dei dati contenuti nei server utilizzati dagli indagati, abbiano comunicato

che la società *"Raw Data"*, presso la quale sono ospitati i server della classe di indirizzi IP 216.176.180.X (che sono risultati essere di proprietà degli indagati o di persone a loro riconducibili), ha ricevuto la richiesta da parte del cliente di scollegarli dalla rete e spedirglieli.

Dello stesso tenore altra richiesta ricevuta dalla società "Dedispec LLC", presso la quale sono ospitati i server della classe di indirizzi IP 199.15.251.X (che in questo caso invece sono di proprietà del provider e sono stati solamente noleggiati dagli indagati), cui il cliente ha chiesto di scollegarli dalla rete.

Alla luce di quanto detto, risulta pertanto chiaro ed inequivoco il tentativo degli indagati di distruggere le fonti di prova a loro carico che, come descritto, si trovano su un sistema informatico estremamente distribuito ed ubicato in paesi esteri, e non ancora del tutto noto.

Non si può quindi escludere che esistano altri server di gestione della botnet, che non sono stati individuati nel corso delle indagini, o addirittura server di backup che possano permettere agli indagati di ripristinare nel completo il sistema informatico da loro utilizzato fino ad oggi, consentendo loro di proseguire le condotte delittuose che hanno portato avanti per diversi anni.

Orbene , anche tale esigenza cautelare appare adeguatamente tutelata , per le medesime ragioni già evidenziate , solo con l' applicazione della misura cautelare della custodia in carcere , avendo i prevenuti già offerto ampia dimostrazione di una significativa e reale capacità di inquinamento e distruzione delle prove .

Al riguardo pure è emersa la sussistenza di una rete di contatti che consente agli Occhionero di acquisire informazioni riguardo il presente procedimento penale , come ha ampiamente dimostrato l' attività di intercettazione da ultimo registrata , ed una precisa volontà dei medesimi ed in particolare dell' Occhionero Giulio , di conoscerne i particolari ed influenzarne gli esiti, dalchè appare assolutamente necessario recidere anche tali collegamenti attraverso l' applicazione di una misura cautelare che escluda qualsiasi possibilità di contatto .

Rileva , poi, in ultimo il giudicante come nei confronti degli indagati sussista anche il pericolo di fuga che appare fondato oltre che sul dato inconfutabile, che entrambi sono residenti a Londra (GB), dove senza dubbio dispongono di locali e conoscenze che potrebbero facilmente consentire loro di darsi alla fuga, anche dalla circostanza che Francesca Maria OCCHIONERO è cittadina degli Stati Uniti, ove è nata ed ha abitato per anni insieme al fratello ed alla famiglia, e che Giulio OCCHIONERO sta da tempo effettuando colloqui di lavoro con società aventi sede all'estero (cfr. sul punto le intercettazioni telefoniche in atti) e ha già ricevuto manifestazioni di interesse da alcune di esse, per posizioni lavorative in Irlanda, Regno Unito o in Polonia.

In particolare tale esigenza cautelare appare dotata del carattere di un ' intensa attualità soprattutto in relazione alla posizione dell' indagato Occhionero Giulio. ben potendo ragionevolmente ritenersi che questi abbia la possibilità di utilizzare alcuni di questi contatti e opportunità lavorative, per darsi alla fuga trasferendosi all'estero.

D' altro canto l' esigenza lavorativa di Giulio OCCHIONERO è certamente più impellente proprio in ragione della necessità, determinata dal presente procedimento penale , di sottrarsi alle indagini della magistratura italiana .

Si riportano , quindi , sul punto alcune delle conversazioni di interesse .

- alle ore 18:09:55 del giorno 08.08.2016, Giulio OCCHIONERO comunica alla madre che gli è stato proposto un lavoro presso la sede di Londra della Deutsche Bank.
- alle ore 18:39:47 del giorno 05.09.2016 Giulio OCCHIONERO riceve una telefonata da un head hunter che gli propone una posizione all'interno di una azienda che ha sede a Dublino.

Si evidenzia come sia emerso più volte nel corso delle indagini, che Giulio OCCHIONERO si è rivolto ad un cosiddetto *head hunter*[29] per trovare un impiego all'estero idoneo alla sua professionalità.

---

29 *Head hunter* è un termine informale per indicare chi svolge la professione di *executive search*, ossia chi effettua ricerca diretta e selezione del personale mirata a trovare i manager più adatti a ricoprire posizioni dirigenziali all'interno di aziende e organizzazioni.

- alle ore 16:13:39 del giorno 09.09.2016 Giulio OCCHIONERO chiama la sorella Francesca Maria e, tra l'altro, la informa che a seguito della visione del certificato ai sensi del 335 C.P., è risultato indagato per i reati di cui all'articolo 617 quater C.P. con P.M. Albamonte.

In tale occasione quindi, Giulio OCCHIONERO è venuto a conoscenza dell'esistenza del presente procedimento penale a suo carico, anche se momentaneamente ipotizza si tratti di querela fatta nei suoi confronti per la rivelazione del contenuto di una email riservata.

- alle ore 16:41:10 del giorno 21.09.2016 Giulio OCCHIONERO racconta alla sorella Francesca Maria di aver ricevuto una telefonata ricevuta dalla Deutsche Bank, che sembrava molto interessata alla sua posizione, e che nei giorni successivi sarebbe stato ricontattato per un colloquio dopodiché, se questo fosse andato bene, sarebbe stato organizzato un incontro presso la loro sede di Londra.

- alle ore 08:39:22 e 08:39:24 del giorno 08.10.2016, ossia tre giorni dopo essere stato sottoposto a perquisizione, riceve le due parti di un messaggio SMS concatenato, inviato dalla TIM, con il quale viene informato che sulla linea è stata attivata l'opzione denominato *Tim in Viaggio Full*, pacchetto che comprende traffico telefonico e telematico da utilizzare in Europa.

Tale attivazione, anche alla luce della particolare circostanza temporale in cui è avvenuta, fa ritenere reale il pericolo che Giulio OCCHIONERO possa darsi alla fuga recandosi all'estero.

- alle ore 23:06:14 del giorno 08/10/2016 Giulio OCCHIONERO riceve un messaggio SMS avente il seguente testo: *"446226 Use this code for Westlands Securit.. verification"*.

Si ritiene che l'aver richiesto, e successivamente ricevuto, tale codice, possa palesare il tentativo di Giulio OCCHIONERO di avere accesso alla rete della *Westlands Securities* (della quale, come descritto, fanno parte i server di gestione del malware), cui evidentemente non riusciva più ad accedere a seguito del sequestro delle *smart card* che utilizzate in precedenza per l'autenticazione.

Un'altra conversazione nella quale viene manifestata la volontà di Giulio OCCHIONERO di trasferirsi all'estero per motivi di lavoro è poi emersa dall'intercettazione telefonica effettuata sull'utenza fissa [redacted] attestata presso la sua abitazione. (vds. Allegato 16)

In data 08.10.2016 infatti, costui ha ricevuto un messaggio SMS dal suo gestore telefonico che gli confermava l'attivazione del servizio *TIM in viaggio Full*, opzione che permette di chiamare e navigare dall'estero a prezzi ridotti.

In conclusione deve quindi affermarsi la sussistenza nei confronti dei due prevenuti delle esigenze cautelari sin qui esposte , sussistendo un concreto ed attuale pericolo di recidivanza , di inquinamento probatorio e di fuga all' estero a fronte dei quali - in ragione delle gravi modalità delle condotte , della loro ripetitività e pervicacia , della loro oggettiva consistenza ed estensione , nonché dell' assenza di strumenti atti a realizzare un efficace controllo nei confronti degli indagati - l'unica misura adeguata appare quella della custodia in carcere .

Né d' altro canto può ritenersi, alla luce delle pene stabilite per le fattispecie così come contestate , e della effettiva gravità delle condotte che la pena che verrà loro inflitta potrà essere contenuta in limiti atti a consentire la concessione del beneficio della sospensione condizionale della pena (al di là della circostanza che allo stato qualsiasi valutazione prognostica appare assolutamente negativa) o comunque entro i tre anni di reclusione così da escludere , ai sensi dell' art. 275 co. 2 bis c.p.p. , l' applicazione della custodia in carcere .

P.Q.M.

Visti gli artt. 272 e ss. e 285 c.p.p.,

APPLICA

Con riferimento ai reati contestati di cui agli artt. 615 ter, commi 1°, 2° n. 3) e 3°, 617 quater, commi 1°, 4° n.1, 617 quinquies, co. 1° 3e 2° (con rif all'art. 617 quater comma 4° n.1) c.p., a

- OCCHIONERO Giulio, nato a Roma [redacted] residente a Londra (GB), ma di fatto domiciliato a Roma in via [redacted]

- OCCHIONERO Francesca Maria, nata a Medford (USA) [redacted] residente a Londra (GB), ma di fatto domiciliata a Roma in via [redacted]

<u>la misura della custodia cautelare in carcere.</u>

Ordina agli ufficiali ed agli agenti di P.G. di procedere alla cattura degli stessi ed alla immediata traduzione dei medesimi presso un istituto di custodia per ivi rimanere a disposizione di questa autorità giudiziaria .

Dispone che dell' esecuzione della misura sia data immediata comunicazione a questa autorità giudiziaria affinchè possa provvedersi tempestivamente agli adempimenti previsti dall' art. 294 c.p.p..

Manda alla Cancelleria per la trasmissione della presente ordinanza in duplice copia all' Ufficio del P.M. per l' esecuzione .

Roma 5 gennaio 2017

Il Giudice
dott. Maria Paola Tomaselli

Maria Paola Tomaselli

Copia conforme all'originale
Roma, 05/01/2017
IL CANCELLIERE
Alessandro Bonucci