



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 se 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

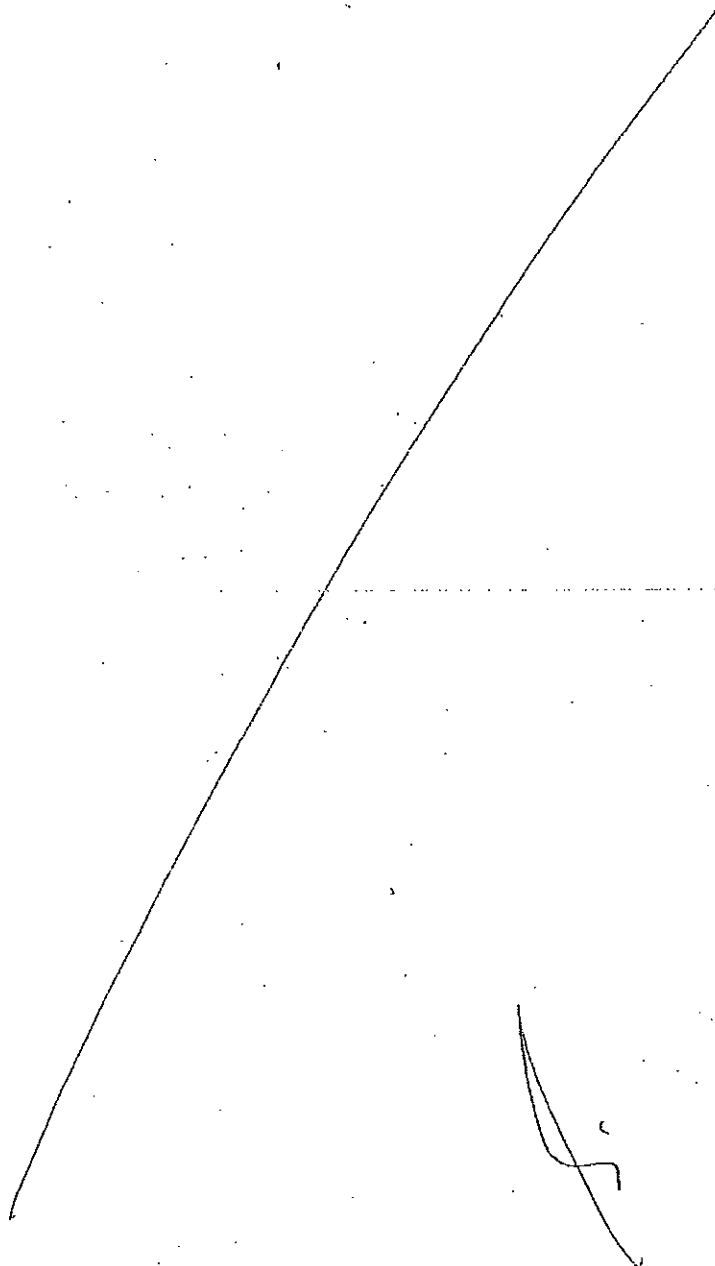
auto - installato nel sistema informatici dell'ENAV S.p.A., avrebbe permesso di accedere abusivamente al relativo sistema informatico, contenente informazioni e dati relativi alla sicurezza pubblica nel settore dell'aviazione civile, nonché di intercettare le comunicazioni informatiche e/o telematiche 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 nonché a numerose autorità politiche e militari di strategica importanza, o di sistemi informatici protetti utilizzati dallo Stato e 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, matteoreenzi.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 utilizzatori 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 Mental Solutions s.r.l. <sup>1</sup> , 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

<sup>1</sup> Società che opera specificamente nel settore della sicurezza informatica 11111111111111

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*<sup>2</sup>, 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*<sup>3</sup>.

<sup>2</sup> 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.

<sup>3</sup> 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

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' *EyePyramid*, 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*<sup>4</sup>.

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)<sup>5</sup> 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 *EyePyramid*<sup>6</sup>, oltre a migliaia di documenti informatici abusivamente esfiltrati secondo la descritta modalità.

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

<sup>5</sup> 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 carpati.

<sup>6</sup> 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* 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-D8102F401003102110C5114F1F18-0E8CF<sup>8</sup>.

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<sup>9</sup>, 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.

<sup>7</sup> 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 (Délaware).

<sup>8</sup> 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.

<sup>9</sup> 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<sup>10</sup>.

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 carpiri dalle macchine compromesse venivano inviati ai seguenti indirizzi email: *purge626@gmail.com*<sup>11</sup>, *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<sup>12</sup>) 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).

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

<sup>11</sup> 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

<sup>12</sup> OSINT, acronimo di Open Source INTeelligence, 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<sup>13</sup> 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 malware, 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*<sup>14</sup>, *eyepiramid.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 *Asterlogic 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

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

<sup>14</sup> 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"<sup>15</sup> 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 utilizzata 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<sup>16</sup> ed accesso ai servizi di directory LDAP<sup>17</sup>), la condivisione di file con protocollo SMB e SMB2<sup>18</sup>, i servizi di posta elettronica<sup>19</sup>, oltre ad un server WEB.

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

<sup>16</sup> 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 "Dedispac 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.enasrl.com,*  
*www.eurecoove.com, www.ayaxisfitness.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<sup>20</sup>.

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*.

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

<sup>18</sup> 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

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

<sup>20</sup> 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<sup>21</sup> 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.*)

<sup>21</sup> 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]	

Stefano	Caldoro	stefanocaldoro [REDACTED]	Parlamentare PdL XI e XVI Legislat. ed ex Ministro Istruzione 2001-2004
Domenico	Gramazio	segreteria [REDACTED]	Parlamentare AN XII e XII Legislat. e Senatore PdL XV e XVI Legislat.
Giovanni	Lucianelli	giovanni.lucianelli [REDACTED] [REDACTED]	ex add. stampa del Sen. De Gregorio
Claudio	Barbaro	barbaro_c [REDACTED]	Parlamentare PdL XVI Legislatura
Roberto	Spinelli	roberto.spinelli [REDACTED]	ex Ambasciatore d'Italia in Messico
Vincenzo Mario	D'Ascola	vincenzomario.dascola [REDACTED] [REDACTED]	
Vincenzo Mario	D'Ascola	nicodascola [REDACTED]	Senatore XVII Legislatura (prima PdL poi AP)
Alessandro	Carino	alessandro.carino [REDACTED]	
Carla Angelica	Maffi	carlaangelica.maffi [REDACTED] [REDACTED]	Ex Dirig. Amministrativo della Procura Generale di Brescia
Maria Gabriella	Marsullo	mariagabriella.marsullo [REDACTED] [REDACTED]	
Armando	Forgione	segreteria.direttore.op [REDACTED] [REDACTED]	Direttore Ufficio Ordine Pubblico del Dipartimento della P.S.
Armando	Forgione	armando.forgione [REDACTED] [REDACTED]	

Si fa inoltre presente che molti degli account presenti nel database, benché privi di password, appartengano a domini di importanti società private o enti istituzionali, quali ad esempio:

- 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*

- ⊙ 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@virgil io.it
fabrizio.sacomanni@[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@inwin d.it
vincenzo.scotti[REDACTED]	05/07/2016 22:57	22/06/2016 06:20	d.latagliata@live.c om
p.fassinio[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.co m
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.i t
i.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.i t
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.carzio [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.cccdb", 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*



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

2) *MDaemon*: contiene i file di configurazione del demone<sup>22</sup> di posta elettronica utilizzato per la gestione dei dati carpati 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:

<sup>22</sup> 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 DA7E17F2" 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-8992671-00524 F0CF4FED" 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<sup>23</sup> 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

<sup>23</sup> 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</a

ction\_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>xHwWtQM</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@stadio[redacted].it</email>

<display\_name>Avv. Daniele Pacioni</display\_name>

<account\_name>Daniele Pacioni</account\_name>

<pop3\_server>pop3.stadio[redacted].it</pop3\_server>

<pop3\_user>daniele.pacioni@stadio[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 gph*: 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).