# TorrentLocker – Enti Italiani sotto riscatto

***Paolo DAL CHECCO, Giuseppe DEZZANI***
***Studio "DIgital Forensics Bureau" di Torino***

***20 ottobre 2014***

Da mercoledì 15 ottobre stiamo monitorando un massiccio attacco informatico a reti di enti Italiani, riceviamo chiamate da Sindaci e Uffici Tecnici di svariati Comuni di tutta Italia ed Enti in generale che – conoscendo la nostra esperienza nell'ambito delle indagini digitali – chiedono supporto per risolvere un problema: all'improvviso, buona parte dei documenti presenti nella rete comunale e sui PC sono diventati illeggibili. I PC funzionano, i documenti sono ancora al loro posto ma non si aprono. Nelle cartelle, insieme ai documenti, sono comparsi dei file dal nome preoccupante "DECRYPT_INSTRUCTIONS.html".

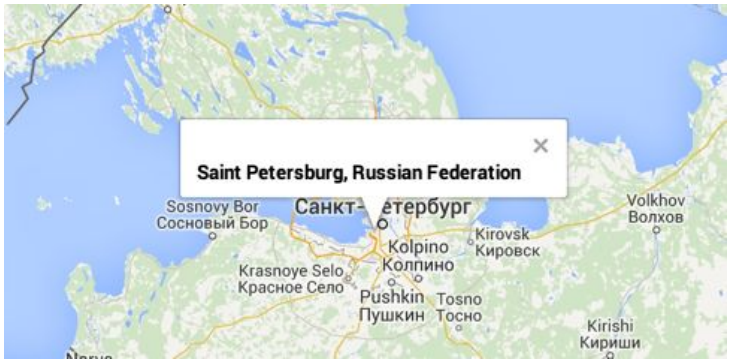
Il danno non si limita ai soli PC, alcuni servizi della rete comunale si sono infatti bloccati, perché i dati su cui i server lavorano non sono più utilizzabili. Il danneggiamento dei documenti ha infatti coinvolto anche diversi aree condivise sulla rete, bloccando gli applicativi che sui documenti facevano affidamento per il regolare svolgimento delle attività comunali.

Avendo ricevuto diverse richieste di supporto per il caso in questione e avendo esperienza in campo di studio di malware, abbiamo proceduto con analisi metodica della compromissione riproducendo più volte su dei nostri sistemi "protetti" le varie fasi dell'infezione analizzando le modifiche al sistema e le comunicazioni Internet. Abbiamo avviato una task force per tentare di illustrare le modalità con le quali prevenire l'infezione e trovare un metodo per decifrare i file che non preveda il pagamento del riscatto.

Anticipiamo, anche se l'analisi verrà svolta nei paragrafi successivi, che abbiamo identificato due degli indirizzi IP sui quali risiede il sistema di controllo dell'organizzazione criminale.

```
01:42:02.147486 IP 46.161.30.20.https > 192.168.0.9.49377: Flags [P.], seq 1:816, ack 167, win 123, length 815
01:42:02.147720 IP 192.168.0.9.49377 > 46.161.30.20.https: Flags [.], ack 816, win 256, length 0
01:42:02.151274 IP 192.168.0.9.49377 > 46.161.30.20.https: Flags [P.], seq 167:525, ack 816, win 256, length 358
01:42:02.302838 IP 46.161.30.20.https > 192.168.0.9.49377: Flags [P.], seq 816:907, ack 525, win 131, length 91
01:42:02.303485 IP 192.168.0.9.49377 > 46.161.30.20.https: Flags [.], ack 907, win 255, length 0
01:42:02.319294 IP 192.168.0.9.49377 > 46.161.30.20.https: Flags [P.], seq 525:834, ack 907, win 255, length 309
01:42:02.482921 IP 46.161.30.20.https > 192.168.0.9.49377: Flags [.], seq 907:2293, ack 834, win 140, length 1386
01:42:02.483106 IP 46.161.30.20.https > 192.168.0.9.49377: Flags [.], seq 2293:2359, ack 834, win 140, length 66
01:42:02.483210 IP 192.168.0.9.49377 > 46.161.30.20.https: Flags [.], ack 2293, win 259, length 0
01:42:02.483275 IP 192.168.0.9.49377 > 46.161.30.20.https: Flags [.], ack 2359, win 259, length 0
01:42:02.487399 IP 46.161.30.20.https > 192.168.0.9.49377: Flags [.], seq 2359:3745, ack 834, win 140, length 1386
01:42:02.487596 IP 46.161.30.20.https > 192.168.0.9.49377: Flags [.], seq 3745:3811, ack 834, win 140, length 66
01:42:02.487607 IP 192.168.0.9.49377 > 46.161.30.20.https: Flags [.], ack 3745, win 259, length 0
```

Riportiamo sopra un estratto della comunicazione di una macchina infettata con il server di controllo che fornisce la chiave di cifratura per crittografare i documenti. Tramite servizi di geolocalizzazione e informazioni provenienti dai dati di registrazione dell'indirizzo IP possiamo identificare la zona in cui risiede il centro di controllo come San Pietroburgo, in Russia.




Questa nuova ondata di infezioni risulta essere stata lanciata lunedì 13 e arrivata in Italia mercoledì 15. In particolare, oltre a indirizzi di privati cittadini o aziende, risultano essere stati coinvolti diversi Uffici Comunali poiché la mail contenente il link al trojan è stata inviata a indirizzi facenti parte della rete dei comuni italiani. Poiché il trojan nei primi giorni di vita non viene rilevato dagli antivirus, da mercoledì ha mietuto migliaia di vittime. Non tutti hanno pagato il riscatto: chi aveva una copia di sicurezza a disposizione la ha ripristinata mentre altri hanno deciso di mettersi l'animo in pace e cercare di ricostruire i documenti persi.

Alcuni antivirus cominciano ora a riconoscere il programma malevolo e impedirne l'avvio e il download. Il problema è che soltanto il 20% di essi è stato aggiornato con la nuova minaccia, chi ha il restante 80% di antivirus o pggio ancora ne è sprovvisto è ad alto rischio di infezione.

Il trojan, che fa parte della categoria dei "ransomware" (software che chiedono un riscatto, "ransom", in inglese) mostra una via d'uscita, dopo avere infettato il PC e reso inutilizzabili i documenti. Pagare 400 euro entro tre giorni, trascorsi i quali il "riscatto" raddoppia raggiungendo gli 800 euro. Il pagamento può avvenire soltanto tramite la nuova valuta digitale Bitcoin, non tracciabile e per questo motivo ideale per attività illecite. Nelle informazioni che il trojan fornisce vi sono persino le istruzioni che spiegano alle vittime come aprire un Wallet Bitcoin (un portafoglio per mantenere la propria valuta), come acquistare il corrispondente in Bitcoin dei 400 euro del riscatto e come eseguire il pagamento all'indirizzo Bitcoin del delinquente (una sorta di IBAN, per intenderci). Una volta ottenuta la "ricevuta" di pagamento (un identificativo della transazione eseguita) il delinquente spiega come comunicargli i

dati e ricevere così il software "antidoto" per decifrare tutti i propri documenti e poterli quindi nuovamente utilizzare.

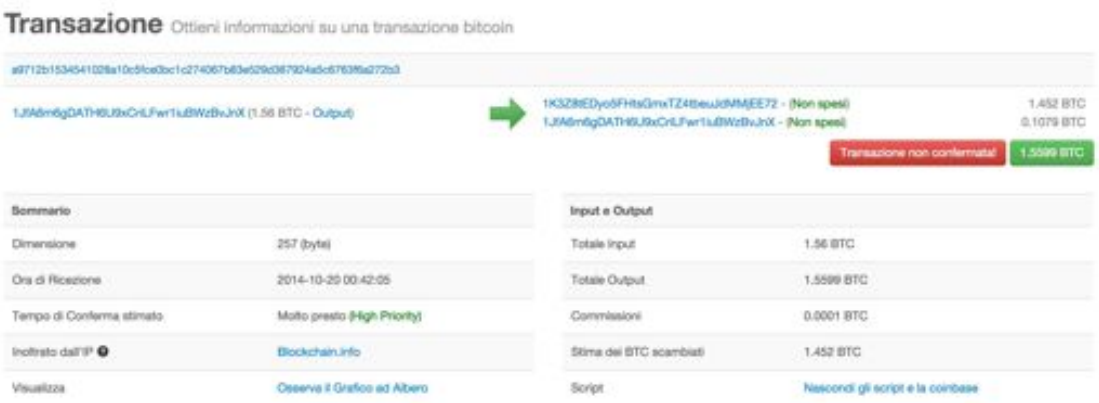
I Bitcoin non sono tracciabili, è vero, ma paradossalmente sono il sistema economico più aperto e pubblico che esista, tanto che è possibile per chiunque verificare quali transazioni sono in corso su un dato indirizzo Bitcoin, cioè su quella sorta di IBAN che il delinquente fornisce per il pagamento del riscatto. Al momento abbiamo identificato due indirizzi Bitcoin utilizzati dai delinquenti per il pagamento, possiamo quindi "spiare" (in modo del tutto legale perché sono pubbliche) le transazioni che vengono emesse nei loro confronti e studiarne l'andamento e le cifre. Vediamo ad esempio il grafico dei guadagni di uno dei due indirizzi Bitcoin: notiamo che prima del 14 ottobre non vi sono stati movimenti, mentre da mercoledì 15 hanno cominciato ad arrivare pagamenti di riscatto con un picco giovedì 16.

Di che cifre stiamo parlando? Da martedì 14 ottobre, in cinque giorni e nei soli due indirizzi Bitcoin da noi identificati (potrebbero esservene anche altri) possiamo contare quasi 100.000 dollari. Il trojan ha diverse varianti e potrebbero essere stati utilizzati altri conti. Purtroppo, il sistema economico dei Bitcoin prevede che le transazioni e gli indirizzi (una sorta di IBAN) siano pubblici, ma non vi sia modo di attribuire un indirizzo a un nome. Potremo seguire quindi nel tempo i guadagni del delinquente senza sapere chi si cela dietro quella sorta di IBAN.

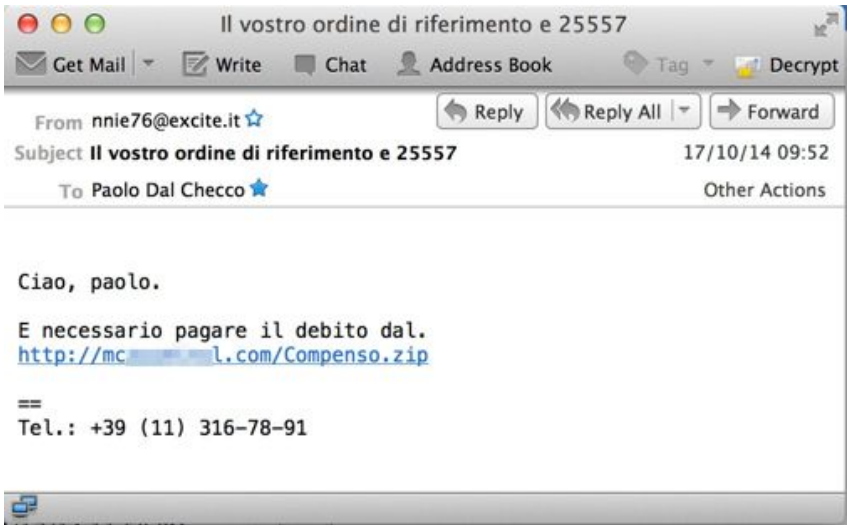
Potete osservare direttamente l'andamento dei due indirizzi bitcoin ai seguenti link:

- https://blockchain.info/address/199EgrnuLeGKXSbimYgbu2MubF2aCYxwNk
- https://blockchain.info/address/1K3Z8tEDyo5FHtsGmxTZ4tbeuJdMMjEE72

Notiamo ad esempio che nel secondo indirizzo bitcoin vi è un pagamento recente di 1.56 Bitcoin, corrispondente all'incirca (la valuta cambia velocemente) alla cifra del riscatto, di lunedì 20 ottobre poco dopo la mezzanotte.

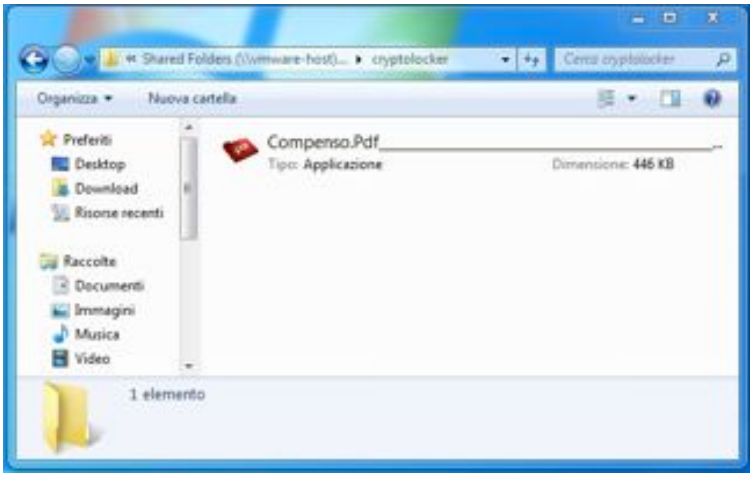



Come ci si infetta? L'attacco arriva tramite messaggi di posta elettronica che contengono riferimenti a fatture di acquisto o debiti da pagare. Ne riportiamo un esempio, ricevuto in una delle nostre caselle di posta elettronica.




Abbiamo cancellato parte dell'indirizzo che viene mostrato nella mail perché da lì è ancora scaricabile ad oggi il trojan e non vogliamo che incauti lettori corrano il rischio di infettarsi scaricando il file.

Il messaggio invoglia chi lo riceve a cliccare perché ci si chiede di quale debito si tratti, colti magari da dubbi o timori. Una volta scaricato il file – un archivio ZIP compresso – al suo interno si trova un documento che a prima vista sembra un PDF.




L'icona ricorda quella dei PDF e il file si intitola "Compenso.Pdf", con una riga che continua dopo il testo "Pdf" fino a uscire dalla schermata, cosa cui magari i più potrebbero non prestare attenzione. Il problema è che in realtà il file è un programma eseguibile: la riga dopo quella che sembra essere un'estensione che indica il tipo di file "pdf" serve infatti per allontanare il più possibile la vera tipologia, cioè "exe". Il vero nome del file è infatti "Compenso.Pdf_____ _____.exe", si tratta quindi in tutto e per tutto di un programma, non di un documento PDF. Buona parte degli utenti saranno invece convinti di avere a che fare con un documento PDF contenente magari una fattura da pagare e lo apriranno.

Per un po' non succederà nulla, poi comparirà la richiesta di confermare l'esecuzione di un software come Amministratore ma sarà già troppo tardi: che lo si confermi o meno il trojan ha già agito eliminando tutti i documenti e convertendoli con una versione codificata e illeggibile, mostrando quindi sullo schermo una preoccupante schermata.

Contemporaneamente, notiamo comparire una finestra che riteniamo essere dovuta al fatto che sui sistemi di test da noi utilizzati per sperimentare l'infezione non era configurato alcun programma di posta elettronica.

Il trojan sta presumibilmente cercando di accedere alla rubrica dei contatti email per propagarsi utilizzando un canale "fidato", sapendo che quando i nostri conoscenti ricevono mail da noi è probabile che siano meno attenti e prevenuti nell'aprire allegati o scaricare link.

I documenti non sono cancellati, sono criptati, cioè resi illeggibili e codificati tramite un algoritmo a chiave simmetrica chiamato AES (lo stesso approvato dall'NSA americana). Ce ne accorgiamo perché se proviamo ad aprirli il sistema dice che sono corrotti, cioè difettosi, inoltre tutti i nostri file finiscono con la parola "encrypted". La nostra tesi di Laurea, che si chiamava "La mia tesi di Laurea.doc" si chiamerà ora "La mia tesi di Laurea.doc.encrypted" e se vi cliccheremo sopra non si aprirà più.

Il problema è che la chiave con la quale sono stati criptati i documenti – e per chiave in questo caso si intende una sorta di password – è a sua volta criptata tramite

algoritmo a chiave asimmetrica chiamato RSA. La password con la quale sono stati codificati i file, quindi, è ricavabile solamente tramite la chiave privata del Command and Control, cioè del server che viene utilizzato dai delinquenti per pilotare da remoto questo processo di cifratura. Il risultato è che tutti i documenti contenuti sul PC sul quale questo *trojan* attecchisce vengono criptati e diventano inutilizzabili: documenti, pdf, fotografie, testi e persino programmi.

In ogni cartella dove il *trojan* ha trovato documenti da criptare, viene lasciato un file chiamato "DECRYPT_INSTRUCTIONS.html" (che significa "Istruzioni per la Decifratura") che l'utente può aprire per cercare di capire cosa è successo, visualizzando la stessa pagina che compare al termine dell'esecuzione del trojan sul PC sul quale è stato avviato. Questi file sono necessari perché il trojan arriva a criptare anche file all'esterno del PC infetto, basta che siano raggiungibili tramite condivisioni di rete. Potenzialmente, un trojan potrebbe essere in grado di criptare tutti i documenti di una rete se i PC sono interconnessi, includendo anche eventuali server di condivisione file se mal configurati.

Il trojan si presenta come "CryptoLocker", un virus malevolo ben noto di cui una società olandese è anche già riuscita a creare una sorta di antidoto per riappropriarsi dei propri file senza pagare. Dello stesso trojan era poi nata in estate una evoluzione, chiamata "TorrentLocker", per la quale anche era stato sviluppato un sistema di decifratura gratuito. Il problema è che in questo caso questa presentazione è una "maschera", perché il trojan è in realtà una nuova versione di "TorrentLocker" e al momento non vi è antidoto che tenga.

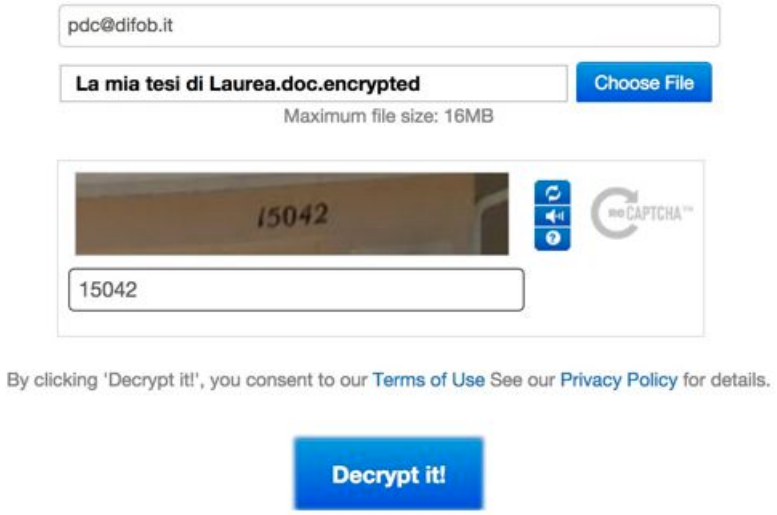
Nella pagina che compare aprendo il documento html, il delinquente che ha sviluppato il trojan spiega come accedere al sito dove è possibile avere informazioni circa le modalità con le quali decriptare i propri file. Per accedere al sito bisogna installare il software TOR, che serve per visitare in anonimato i siti web e allo stesso tempo per poter accedere a siti anonimi ospitati sulla rete TOR, detti "Hidden Services" (servizi nascosti). Accedendo alla pagina nascosta vediamo questo preoccupante messaggio.

Ci viene dato un ultimatum, abbiamo circa tre giorni per pagare 400 euro e poter riutilizzare i nostri documenti, passati i quali il riscatto raddoppia. Per dimostrarci che fa sul serio ed è in grado di decifrare i nostri documenti, il delinquente permette

gratuitamente di decifrare un documento di dimensione inferiore a 1 MByte, cliccando sul link "Decrypt File Singolo – Free".

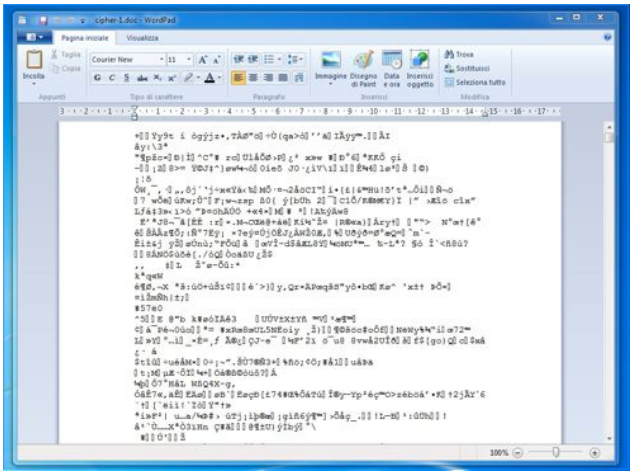
Appurato che il delinquente è in grado di decriptare i file, possiamo provare a utilizzare i due sistemi al momento esistenti per decriptare le vecchie versioni di CryptoLocker e TorrentLocker, sperando che il trojan non sia proprio l'ultima versione.

Visitiamo allora l'indirizzo "www.decryptcryptolocker.com" e carichiamo un file cryptato, inserendo il nostro indirizzo email e confermando che siamo esseri umani digitando il numero che leggiamo nel box.



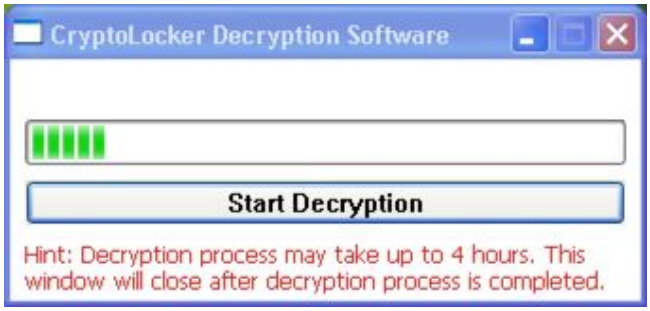

Purtroppo il sito ci dice che la cifratura di questo trojan non è tra quelle che lui è in grado di decifrare.

Proviamo allora a scaricare il software TorrentUnlocker dall'indirizzo "download.bleepingcomputer.com/Nathan/TorrentUnlocker.exe" e lo avviamo. Il software ci chiede di trovare un file criptato di cui possediamo, da qualche parte (magari in un backup o nel Cloud su Dropbox) una versione ancora leggibile, di dimensioni maggiori di 2 MB. In questo modo il programma è in grado di ricavare una possibile chiave di decifratura. Anche in questo caso, purtroppo, non otteniamo nulla perché il software è in grado di decifrare soltanto file cryptati tramite le versioni TorrentLocker di agosto e settembre. Se apriamo il file decryptato, infatti, troveremo soltanto caratteri illeggibili.



A questo punto capiamo che non c'è nulla da fare e, se dei documenti non abbiamo backup (copie di sicurezza) non ci resta che pagare. Procediamo quindi con l'aprire un Wallet Bitcoin, ricaricare il conto con la somma richiesta ed eseguire il versamento sul conto del delinquente, informandolo a pagamento avvenuto. A questo punto, ci verrà indicato il link dove scaricare immediatamente il software con l'antidoto per decriptare i documenti, contenuto all'interno dell'archivio compresso "Decryption_Software.rar". Scompattiamo l'archivio e avviamo il software di decriptazione, che anche in questo caso si maschera come "CryptoLocker" mentre in realtà è una variante.

Avviamo la Decryption e si avvierà l'operazione di decifratura che dipenderà da quanti documenti sono stati criptati.




Al termine del procedimento otterremo la seguente schermata, che ci informa che è necessario riavviare il PC per completare la pulizia del sistema.

In base alle esperienze che ci sono state riportate, in genere i delinquenti forniscono l'antidoto quando ricevono pagamenti – ci sono stati però casi nei quali dopo il pagamento la vittima non ha ricevuto nulla. Tendenzialmente, è interesse delle organizzazioni criminali rispettare la promessa della restituzione dei documenti in cambio del pagamento del riscatto, perché se si diffonde la notizia che il pagamento non serve a nulla, sempre meno vittime cederanno al riscatto e tenteranno di ripristinare i documenti in modi alternativi.

In ultimo, come si può prevenire l'infezione? Anche se tutti gli antivirus non hanno ancora aggiornato i loro database per rilevare questa minaccia, consigliamo comunque di installare un antivirus e mantenerlo il più aggiornato possibile. Senza manifestare preferenze, mostriamo quali – sui 50 antivirus analizzati – sono quelli che ad oggi rilevano la minaccia e proteggono gli utenti dall'infezione.

| Antivirus | Result | Update |
|---|---|---|
| AVG | Zbot.QDU | 20141017 |
| AegisLab | Hoax.W32.ArchSMS | 20141017 |
| Avast | Win32:Malware-gen | 20141017 |
| Avira | TR/Dropper.A.31041 | 20141017 |
| Baidu-International | Trojan.Win32.Filecoder.bDI | 20141016 |
| ESET-NOD32 | Win32/Filecoder.DI | 20141017 |
| Kaspersky | Trojan.Win32.Scarsi.xgd | 20141017 |
| Qihoo-360 | Win32/Trojan.Dropper.0a9 | 20141017 |
| Symantec | Trojan.Cryptolocker.F | 20141017 |
| TrendMicro-HouseCall | Cryp_lspi | 20141017 |

Gli altri antivirus lasciano passare la minaccia e non si accorgono che si tratta di un trojan che può compromettere tutti i documenti dell'utilizzatore del PC e della sua rete. Lentamente, però, tutti i produttori stanno aggiornando le definizioni dei virus e malware dei loro prodotti ed entro qualche giorno saranno probabilmente quasi tutti allineati.

Gli amministratori di sistema possono, inoltre, imporre regole di utilizzo della posta elettronica e del web impedendo il download di file da Internet o filtrandoli, magari tramite applicazione di antivirus/antimalware/sandbox preventivamente.

Ancora, dato che i vettori sono ormai noti, i gestori della rete aziendale potrebbero impostare delle "regole" per bloccare i file prima ancora che vengano scaricati o analizzati dagli antivirus, considerando che magari l'antivirus aziendale potrebbe non rilevare ancora il trojan. Ad oggi abbiamo identificato tre payload, cioè tre vettori di inferzione. Si tratta dei file che vengono scaricati dagli incauti destinatari delle mail dai link contenuti all'interno dei messaggi. Di tali file conosciamo i link nei siti dove sono stati caricati, alcuni sono ancora attivi tutt'oggi ma è probabile che vengano presto disattivati e ne vengano generati di nuovi. Per questo motivo, gli amministratori di sistema possono inserire in blacklist, cioè nella lista dei software da non ammettere, i valori hash dei file malevoli, che sono i seguenti:

- 873de1db4bb2b693eb370d9b28a4c0a5
- 206b5136095cb2bcfb902c8ffb218163
- 11ff8a8e9a643deff1dcf58e7e2fdf20

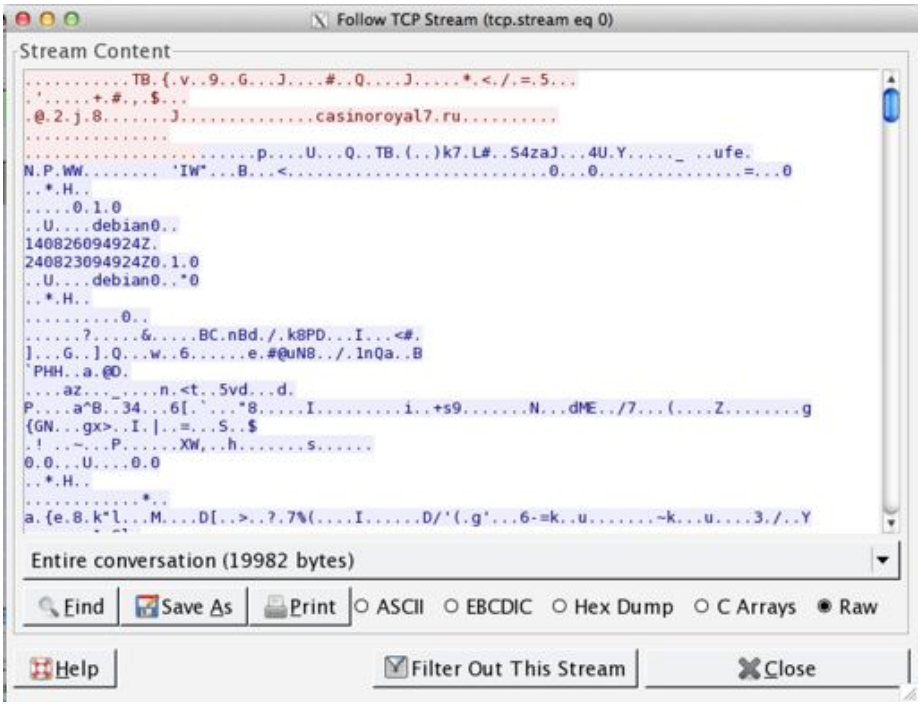
Abbiamo rilevato per ora due indirizzi IP dei server di gestione chiamati "Command and Control". Tali indirizzi possono essere inseriti nei firewall aziendali per bloccare la comunicazione con i sistemi dell'organizzazione criminale. Abbiamo sperimentato che se il PC infetto non riesce a comunicare con i server di controllo, il trojan non ha effetto e si fornisce agli antivirus il tempo di rilevarlo e debellarlo. I due indirizzi IP dei centri di controllo dell'organizzazione rilevati ad oggi sono i seguenti:

- 46.161.30.20
- 46.161.30.16

I due indirizzi IP sono geolocalizzati in Russia e hanno i seguenti dati di registrazione:

```
inetnum:        46.161.30.0 - 46.161.30.255
netname:        KolosokIvan-net
descr:          Net for customer ID 12510
country:        RU
admin-c:        KI811-RIPE
tech-c:         KI811-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-PIN
mnt-by:         MNT-PINSUPPORT
mnt-routes:     MNT-SELECTEL
source:         RIPE # Filtered
```

Analizzando il traffico scambiato tra un PC infetto e il server di controllo, abbiamo notato che all'interno del primo messaggio inviato dal PC vi è un riferimento a un dominio: "casinoroyal7.ru".




Confermiamo che questo dominio punta direttamente all'indirizzo IP del Command & Control. Il dominio risulta essere **registrato martedì 14 ottobre 2014** in modo anonimo, da un utente localizzato a Mosca, quindi l'indagine diventa complessa.

```
domain:         CASINOROYAL7.RU
nserver:        ns1.reg.ru.
nserver:        ns2.reg.ru.
state:          REGISTERED, DELEGATED, UNVERIFIED
person:         Private Person
registrar:      REGRU-RU
admin-contact:  http://www.reg.ru/whois/admin_contact
created:        2014.10.14
paid-till:      2015.10.14
free-date:      2015.11.14
source:         TCI
```

In ultimo, gli utenti dovrebbero ormai sapere che – a meno che non si abbia assoluta certezza della provenienza e del contenuto – non si aprono gli allegati ai messaggi di posta e soprattutto non si scaricano file presenti su indirizzi web indicati nei messaggi.