Ransomware 2017

Italy

Gianfranco
Tonello

Laureato in ingegneria informatica a Padova, CEO di TG Soft Security Software Specialist e direttore del C.R.A.M.

- Ricercatore di Virus/Malware dal 1990 con pubblicazione di analisi presso il VTC |*Virus Test Center*| dell'Università di Amburgo e riviste italiane.
- Sviluppatore software Anti-Malware:
  - dal 1992 VirIT per DOS;
  - dal 1997 Vir.IT eXplorer PRO per Windows®;
  - dal 2013 VirIT Mobile Security per Android™

WildList reporter | www.wildlist.org

Membro AMTSO *Anti-Malware Testing Standards Organization* | www.amtso.org

Membro VIA *Virus Information Alliance di Microsoft*

Membro MVI *Microsoft Virus Initiative*

Gianfranco **Tonello** | C.R.A.M. *Centro Ricerche Anti-Malware*

TG Soft
Security Software Specialist
ANTIVIRUS · ANTISPYWARE · ANTIMALWARE
www.tgsoft.it

C.R.A.M.
CENTRO RICERCHE ANTI-MALWARE

Ransomware 2017

Italy

Analisi dei principali attacchi Ransomware da luglio 2015 a febbraio 2017 in Italia

Autore

Gianfranco Tonello

Autore

Gianfranco Tonello

Ceo di TG Soft, autore di VirIT, Direttore del C.R.A.M., Senior Security Expert

https://it.linkedin.com/in/gianfranco-tonello-77078843

Collaboratori

Enrico Tonello

Ricercatore AntiMalware, Senior Security Evangelist e co-autore di Vir.IT eXplorer PRO

Federico Girotto

Responsabile supporto tecnico TG Soft e amministratore del Virus Lab di VirIT

Claudio Sachespi

TG Soft

Michele Zuin

TG Soft

Indice

Introduzione

Questo rapporto sui ransomware 2017 è stato redatto sulla base dati del *Centro di Ricerca Anti Malware* di TG Soft di seguito indicato sinteticamente con C.R.A.M., con l'obiettivo che il lettore possa trovare utili informazioni per proteggere la propria organizzazione, i propri utenti e dati da questo tipo di minacce.

Il rapporto prende in esame il periodo che va dal 1 gennaio al 31 dicembre 2016, confrontandolo con gli ultimi sei mesi del 2015, di tutti gli attacchi che sono stati riscontrati in Italia e analizzati dal C.R.A.M. in relazione a queste tipologie di minacce.

L'analisi metterà in evidenza l'evoluzione che è stata riscontrata nel 2016 delle varie famiglie di ransomware che si sono diffuse attraverso le svariate campagne che hanno visto come obiettivo anche l'Italia.

Il rapporto oltre ad analizzare le varie famiglie di ransomware che si sono diffuse in Italia, illustrerà approcci e tecnologie euristico-comportamentali per mitigare e proteggersi da queste tipologie di attacchi.

Verranno illustrate le tecnologie, presenti nella suite Vir.IT eXplorer PRO, Anti-Ransomware protezione Crypto-Malware e un sistema di Backup "protetto" in grado di preservare dalla cifratura anche da minacce di nuova generazione.

Il rapporto "Ransomware 2017" è una guida rivolta principalmente agli ICT Security Manager, alle figure professionali dei cybersecurity aziendali, ai sistemisti e a tutti coloro che vogliono proteggersi da questo tipo di minacce.

Ransomware: cosa sono?

Con il termine "Ransomware" definiamo tutti quei programmi o software che bloccano l'accesso ai file di documenti o al computer chiedendo un riscatto in denaro per accedervi.

I ransomware vengono progettati per rendere il computer o i file inutilizzabili, con lo scopo di estorcere denaro alla vittima costringendola al pagamento di un riscatto.

All'inizio i ransomware si limitavano a bloccare l'interazione con il computer, visualizzando una falsa schermata delle forze dell'ordine, dove venivano imputati una serie di violazioni e una richiesta di riscatto, per riottenere l'accesso al computer.

Il più famoso di queste tipologie di ransomware è il *Trojan.Win32.FakeGdF*, la cui prima apparizione risale al 2011, che visualizzava una finta schermata della Guardia di Finanza.

Ransomware: Trojan.Win32.FakeGdF.A

I malware appartenenti alla prima "era" dei ransomware della tipologia dei *Trojan.Win32.FakeGdF* erano facilmente rimuovibili in un modo o nell'altro senza la necessità di pagare il riscatto.

Inoltre, il pagamento del riscatto del Trojan.Win32.FakeGdF, non comportava lo sblocco del computer, ma era solo una vile forma di truffa!

Gli autori di questa tipologia di ransomware non incassarono grandi cifre con il pagamento dei riscatti. Questo però non li scoraggio poiché modificarono il loro obiettivo.

Cosa c'è di più importante se non i documenti di lavoro, i database e gli archivi aziendali, le foto più care, devono aver pensato i cyber-criminali. E se queste venissero cifrati con algoritmi estremamente forti, come AES o RSA, rendendo impossibile la loro decifratura, a meno che non si conosca la password. Le vittime colpite sarebbero state costrette a pagare il riscatto, a meno che…

Verso la fine del 2012 una nuova forma di ransomware fece la sua apparizione, quella chiamata con il nome di Crypto-Malware.

I ransomware si possono suddividere in 2 gruppi:

- Trojan.Win32.FakeGdF (blocco del computer)
- Crypto-Malware (cifratura dei file)

Per maggiori informazioni sui ransomware che prendono in ostaggio il computer:

03/12/2010 - Una nuova minaccia prende in ostaggio il computer chiedendo 100$ per rilasciarlo

14/12/2011 - Trojan.Win32.FakeGdF.A

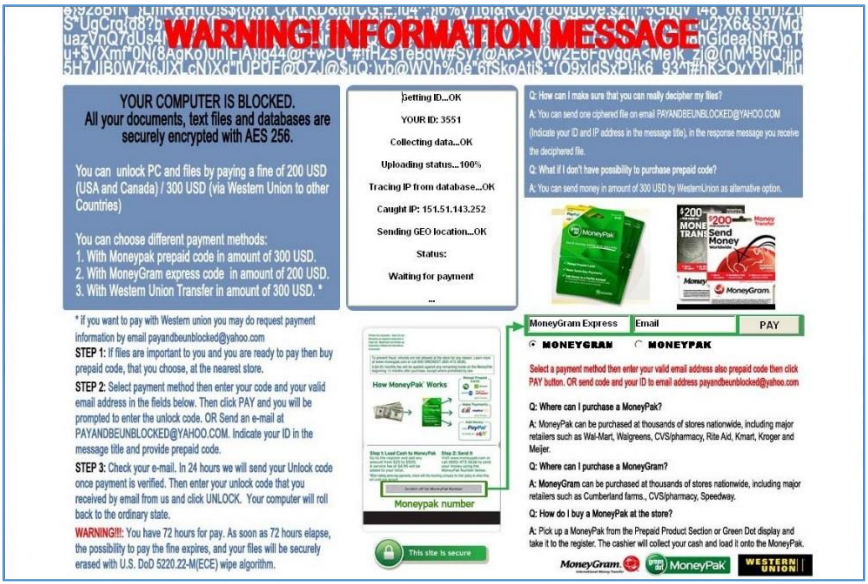
15/11/2012 - Come difendersi dal Trojan.Win32.FakeGdF e dalle sue numerose varianti (Virus della Guardia di Finanza, della Polizia di Stato, della SIAE etc. etc.)

L'era dei Crypto-Malware

Con il termine di Crypto-Malware definiamo tutti quei ransomware che vanno a cifrare i file di documenti o dati attraverso una chiave (password), rendendo impossibile l'accesso fino al pagamento di un riscatto in denaro (Bitcoin).

Il capostipite dei Crypto-Malware è stato il ransomware DocEncrypter (info CRAM 509), la cui prima apparizione risale a dicembre 2012.

Si tratta di un ransomware ibrido, perché andava sia a bloccare l'accesso al computer, analogamente al FakeGdF, sia a cifrare i file documento (.rtf, .txt, .chm, .jpg e altri formati) rendendoli inutilizzabili aggiungendovi l'estensione "*.block*".



Riscatto richiesto dal DocEnCrypter

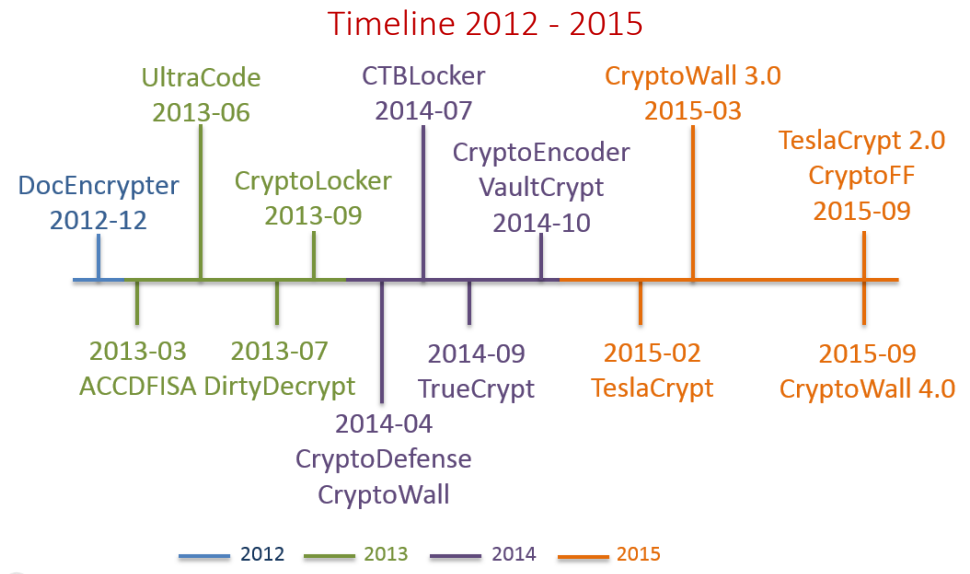
A luglio 2013 viene scoperto un nuovo ransomware chiamato DirtyDecrypt (info CRAM 542), come il DocEncrypter, oltre a bloccare l'accesso al computer, va a cifrare i file di documento chiedendone un riscatto.

Sicuramente il ransomware più famoso al mondo è il CryptoLocker, la cui prima apparizione risale a settembre 2013. Il CryptoLocker è divenuto così famoso, che molti media, identificano con questo nome qualsiasi ransomware che cifra file di documenti.

CryptoLocker non è il solo unico ransomware ad aver ottenuto una fama internazionale, altri malware sono stati sviluppati nei mesi e anni successivi. Ad esempio nel 2014 ad aprile si diffonde CryptoWall e a seguire nel mese di luglio il CTBLocker (info CRAM 608).

Nel 2015 fa la sua prima apparizione nel mese di febbraio TeslaCrypt. Nei mesi successivi troviamo nuove versioni di CryptoWall, la 3.0 a marzo e successivamente, a settembre, vengono rilasciate le versioni 2.0 di TeslaCrypt e 4.0 di CryptoWall.

Di seguito nell'immagine riportiamo la Timeline 2012-2015:



Nel 2016 si riscontra un vera e propria esplosione nello sviluppo di nuovi ransomware.

A metà gennaio fa l'apparizione la versione 3.0 di TeslaCrypt, che verrà ricordata per il lunedì nero del 1° febbraio 2016, dove si toccò l'apice dell'attacco da parte di questa famiglia di crypto-malware.

Ma a febbraio, oltre all'attacco del TeslaCrypt, viene rilasciato un nuovo ransomware chiamato Locky (info CRAM 698), che diverrà nei mesi successivi lo spauracchio degli istituti ospedalieri americani e non solo.

A marzo nuovi ransomware spuntano come funghi: Cerber (info CRAM 707), Rokku (info CRAM 706), HydraCrypt (CryptoXXX) (info CRAM 715) e Petya. Un piccolo inciso su Petya, si tratta di un ransomware 2.0 per le sue particolare tecniche innovative, poiché cifra la Master File Table di ogni disco, rendendo impossibile l'accesso alle unità.

Ad aprile troviamo il malware Maktub, che per il suo layout molto ricercato graficamente potremmo definirlo come un ransomware "artistico".

A maggio viene rilasciato Petya 2, il quale incorpora anche il ransomware Mischa. Sempre in questo mese troviamo i primi ransomware della famiglia CrySis, come Saraswati (info CRAM 723).

A giugno si diffonde Satana e Locky si trasforma in Zepto (info CRAM 737).

A luglio viene rilasciato Petya 3 e CryptoXXX si trasforma in CryptoPPP.

Ad agosto vengono rilasciati Cerber 2 e 3, seguiti da ransomware ispirati a *Mr. Robot* come FSociety e a PokemonGo.

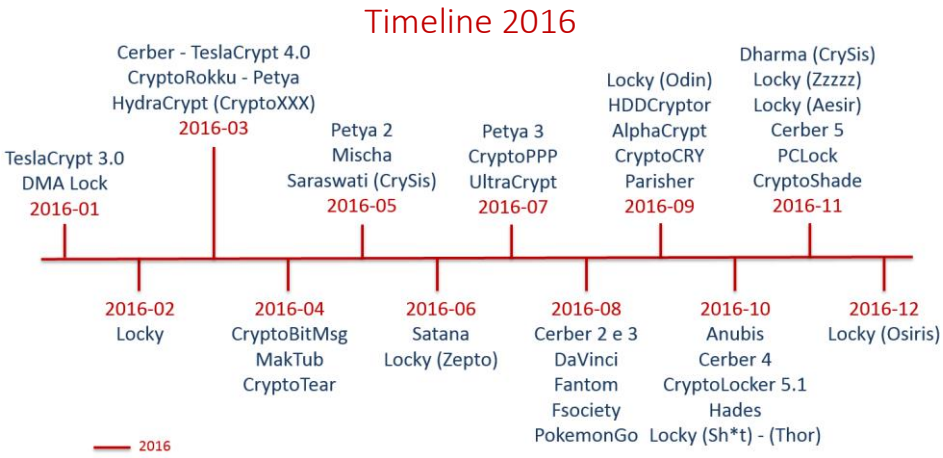
A settembre si riscontrano attacchi di una nuova release Locky, che cifra i file aggiungendo l'estensione Odin. Sempre a settembre fa la sua comparsa il ransomware HDDCryptor che segue le orme di Petya, andando a cifrare il contenuto del disco attraverso un tool opensource.

A ottobre arriva dall'Egitto il ransomware Anubis (info CRAM 763), la versione 4 di Cerber, il CryptoLocker 5.1 made in Italy e 2 nuove versioni di Locky (Sh*it e Thor).

A novembre troviamo Dharma appartenente alla famiglia CrySis, Cerber 5, CryptoShade (info CRAM 817) e 2 nuove varianti di Locky.

A dicembre continua lo sviluppo incessante di Locky con la variante Osiris.

Di seguito si può osservare la Timeline grafica dei Ransomware realmente circolanti in Italia nel 2016.



Nei primi 2 mesi del 2017 sono state identificate le seguenti nuove tipologie di ransomware: Globe, Sage, Spora, Merry X-mas, CryptoShield, Renamer e CryptoFAG. Interessante è il ransomware "Renamer", il quale non cifra il contenuto dei file ma ne rinomina il nome aggiungendovi come prefisso "*unCrypte@INDIA.COM_*" seguito dal nome del file originale cifrato con l'algoritmo AES256:
https://www.tgsoft.it/italy/news_archivio.asp?id=795 .

Metodi di diffusione

I metodi di diffusione utilizzati dai ransomware sono i medesimi delle altre tipologie di malware:

- Via email
- Navigazione su siti infetti
- Altri malware
- In bundle con altri software
- Attacco via Desktop remoto

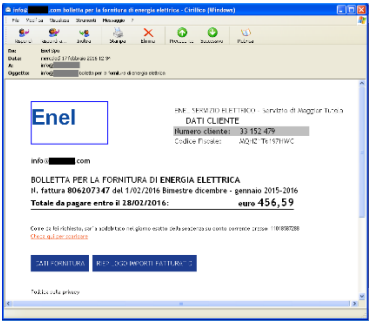
Vettore d'infezione: posta elettronica

Il vettore di infezione più utilizzato rimane la posta elettronica, dove viene sfruttata l'ingegneria sociale, per indurre la malcapitata vittima ad eseguire l'allegato infetto oppure a cliccare sul link presente all'interno del corpo del messaggio.

Casi eclatanti sono state le finte bollette di Telecom o Enel, il finto pacco del corriere SDA oppure l'avviso di pagamento di Equitalia, che hanno veicolato il ransomware CryptoLocker o altre tipologie.

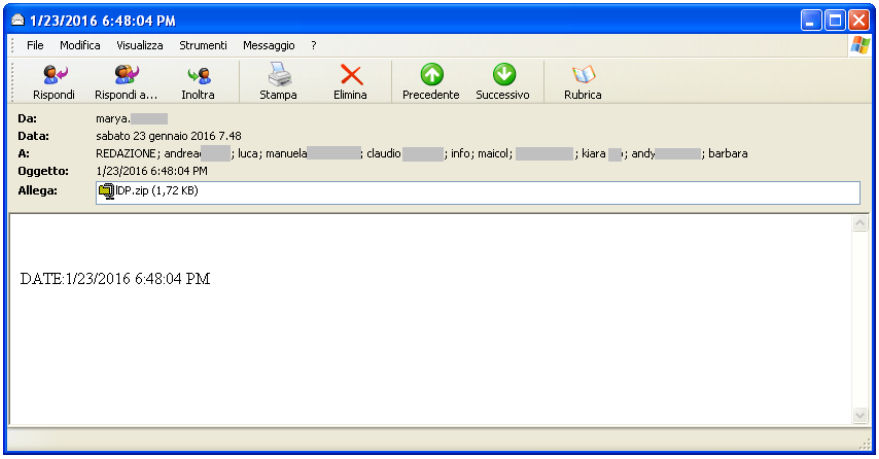
In altri casi l'email arrivava da un contatto conosciuto, noto al destinatario, come già utilizzato nella tecnica di spoofing, questo induce la malcapitata vittima a pensare che il messaggio sia realmente inviato dal proprio conoscente e non da un malfattore.

In figura possiamo vedere la finta bolletta dell'Enel, che al suo interno contiene un link per scaricare la fattura che porta l'utente su un sito malevolo:



Nell'immagine sottostante si può notare il finto sito dell'ENEL da dove vengono scaricate varianti di CryptoLocker:

Un altro esempio di diffusione via e-mail, forse il più eclatante, è avvenuto tra fine gennaio e inizio febbraio 2016. Si tratta di TeslaCrypt 3.0 che, per diffondersi, ha utilizzato un invio massivo di oltre 45 milioni di e-mail con in allegato il file .ZIP contenente questo temibilissimo ransomware. Per l'invio sono stati utilizzati 4000 account SMTP compromessi:



Vettore d'infezione: siti compromessi

Altro metodo utilizzato come vettore d'infezione è la navigazione su siti compromessi o siti esca, legittimi o no, che contengono script malevoli o sfruttano vulnerabilità di Java, Adobe Reader o Adobe Flash, per inoculare il ransomware nel computer della vittima.

Anche la visualizzazione di banner pubblicitari, distribuiti da alcuni importanti network di advertisement, sono stati utilizzati per veicolare infezioni di ransomware.

Vengono utilizzati "exploit kit" per infettare i siti ed eseguire download automatici di malware. Gli exploit kit più utilizzati sono:

Neutrino	Angler (alias Axpergle)
Magnitude	Nuclear Pack
Rig (alias Meadgive)	Empire Pack

La rete "botnet" dei siti compromessi da questi "exploit kit" viene affittata per un determinato periodo a qualche malfattore, per veicolare i propri malware. Può succedere che in fasce diverse della giornata siano diffuse più versioni differenti di malware, dai ransomware ai Trojan.Banker.

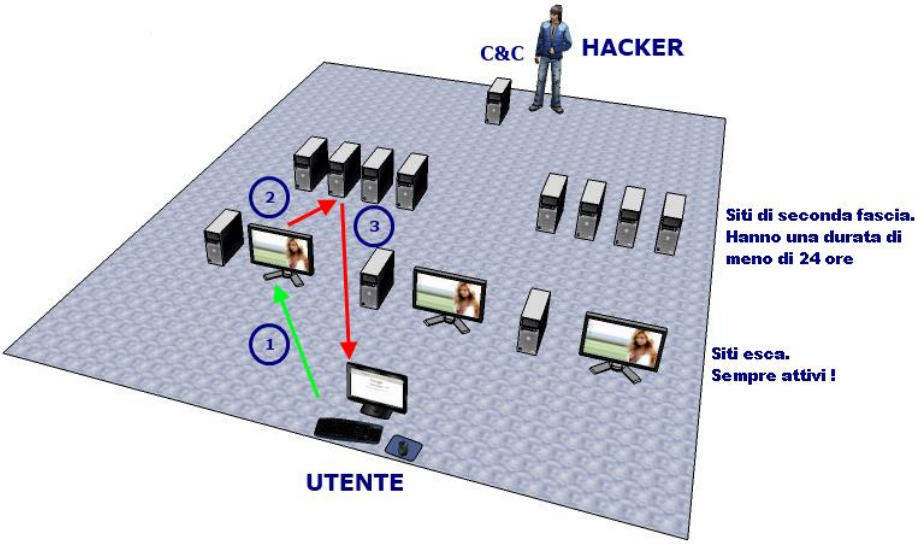
Ad esempio l'exploit kit Magnitude nel 2014 distribuiva oltre al trojan Banker *Zeus*, il ransomware CryptoWall.

L'exploit kit Neutrino è stato utilizzato da Locky (febbraio 2016), da TeslaCrypt (marzo 2016) e dal Cerber (marzo 2016) come vettore d'infezione.

Angler EK è stato utilizzato da CryptoXXX a partire da marzo 2016, ma anche da TeslaCrypt. Invece Nuclear Pack è stato utilizzato da Locky sempre a partire da marzo 2016.

Rig EK ha distribuito la versione Odin di Locky (settembre 2016), il Cerber (ottobre 2016) e altre famiglie di ransomware.

Nell'immagine sottostante è rappresentata un'infrastruttura che comprende i siti esca per la diffusione di ransomware.

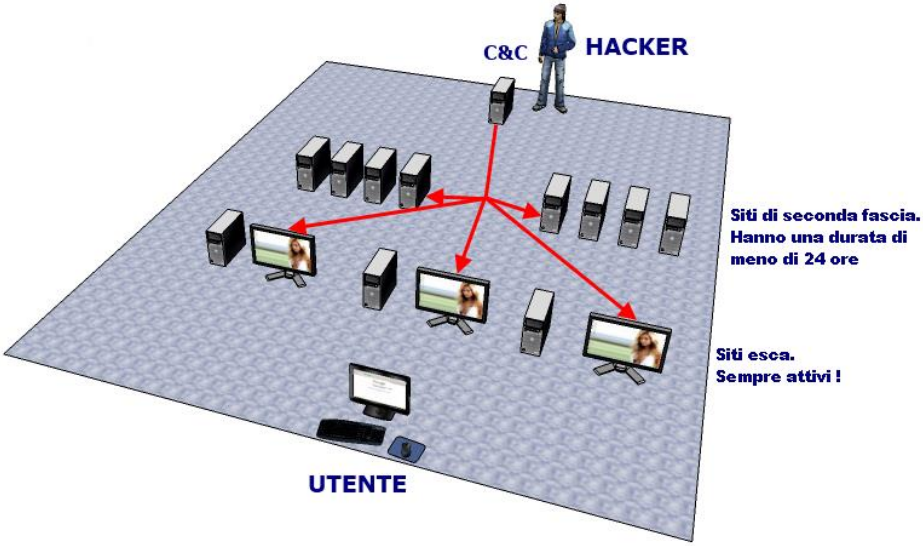


1. L'utente navigando in internet, finisce per collegarsi ad un sito per adulti, generalmente creato ad hoc (sito esca).
2. Il sito esca esegue un redirect ad un altro server su un sito che chiameremo di "seconda fascia". I siti di seconda fascia hanno una vita molto breve, questi domini, generalmente, non restano online per più di 24 ore utilizzando la tecnica DGA (domain generation algorithm).
3. Il sito di seconda fascia, inizierà a comunicare con il computer dell'utente, inviando archivi Java/PDF/Flash con exploit kit e file eseguibili/dll contenenti il ransomware.

I siti "esca", sono domini sempre attivi che sono stati compromessi oppure creati ad hoc dagli autori di questa truffa.

I siti di "seconda fascia" sono domini che durano meno di 24 ore, su questi server sono memorizzate le componenti del malware e/o statistiche d'infezione.

Nell'immagine sottostante lo schema di gestione dei siti "esca" e dei domini di "seconda fascia" attraverso il server di Comando&Controllo gestito dall'hacker.



Può succedere che il sito "esca" memorizzi l'indirizzo IP dell'utente, nel caso che questo utente sia già stato infettato, non verrà eseguito il re-indirizzamento al sito di "seconda fascia" per l'infezione, ma verrà visualizzato l'agognato sito per adulti.

Nel caso di siti legittimi ma compromessi, l'exploit kit re-indirizzerà il download del ransomware direttamente ai siti di "seconda fascia" generati con la tecnica DGA.

Vettore d'infezione: altri malware

Vi sono particolari sotto-famiglie di trojan, che fungono da dropper o downloader di altri software malevoli. Come gli exploit kit, queste tipologie di trojan, affittano la propria botnet al malfattore, per infettare il computer della vittima con altri malware, come i ransomware.

In questo modo si sfrutta il vantaggio che il malware "dropper" si trova già all'interno del computer della vittima.

Esempi di trojan dropper/downloader:

- SathurBot
- HydraBot

Tra il 2015 e il 2016 la botnet di SathurBot è stata affittata per distribuire ransomware come: CryptoWall, CryptoEncoder, HydraCrypt (CryptoXXX) e altri.

Invece HydraBot è stata utilizzata nel 2016 per distribuire Cerber, PCLock (info CRAM 770) e altri ransomware. Cerber, ad esempio, è stato diffuso da HydraBot in modo intermittente con frequenza di 2/3 giorni dove la botnet quando non scaricava Cerber diffondeva altri malware come Kovter, Miuref, BrowseMe e altri meno noti.

HydraBot utilizza un client di Torrent per diffondersi tra le vittime, andando a condividere falsi film "esca", come ad esempio: "*Jason Bourne 2016.avi*", "*Inferno 2016.avi*", "*Guardians of the Galaxy Vol. 2 2017.avi*", etc.
All'interno del pacchetto scaricato via Torrent, oltre al film è presente anche un software di codec "*Ultra XVid Codec Pack.exe*". L'apertura del film con un qualsiasi programma di media player visualizza il messaggio di errore "codec non supportato", in modo da indurre la vittima ad eseguire il malware contenuto nel programma eseguibile "Ultra XVid Codec Pack.exe" da cui infetterà l'utente con HydraBot.

Vettore d'infezione: in bundle con altri software

Negli ultimi mesi si sta diffondendo un nuovo approccio di vettore d'infezione, utilizzando software legittimi per veicolare l'infezione, inserendovi all'interno software malevolo.

Questa tecnica di mettere in bundle il malware all'interno di software "buoni", prelevati direttamente dal sito del produttore o del distributore, nel 2016 ha permesso di veicolare ransomware, ma anche malware classificati come APT (Advanced Persistent Threat).

Nell'estate del 2016 eclatante è stato il caso del software Ammyy, programma di assistenza remota, che in determinate fasce orarie dal sito del produttore, vi era la possibilità di scaricare il software di installazione di Ammyy infetto dal ransomware Cerber. Chi installava tale versione, eseguiva in parallelo il ransomware Cerber e il programma di installazione originale di Ammyy (info CRAM 751).

Ammyy non è nuovo a questo tipo attacco, già negli anni precedenti aveva distribuito altre famiglie di malware.

Vettore d'infezione: attacco via desktop remoto (RDP)

Un altro metodo di diffusione di ransomware, che è stato riscontrato negli ultimi anni è l'attacco al desktop remoto. Questa tipologia di attacco consiste nel "loggarsi" al computer con le credenziali della vittima e di eseguire il ransomware manualmente sul computer.

Il malfattore esegue un attacco "brute force" per determinare le password degli utenti utilizzate per accedere al server via Desktop Remoto. Nei casi di attacco si sono riscontrati accessi sia come utente "guest", sia come "Administrator" o altri user. Quando il malfattore riesce ad accedere al server con l'utente "Administrator" crea nuovi utenti all'interno del server. Quindi è vitale disabilitare l'utente "guest" e utilizzare password robuste

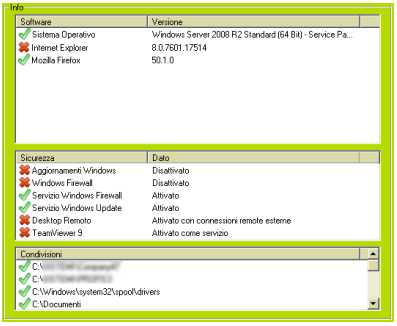
(non riconducibili al nome dell'utente). Se l'azienda non usa il servizio di desktop remoto questo va disabilitato.

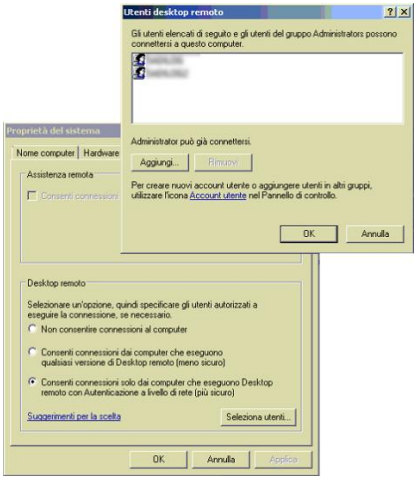
Vediamo ora un caso reale di attacco ad un server Windows 2008 R2 da parte del ransomware CrySis.

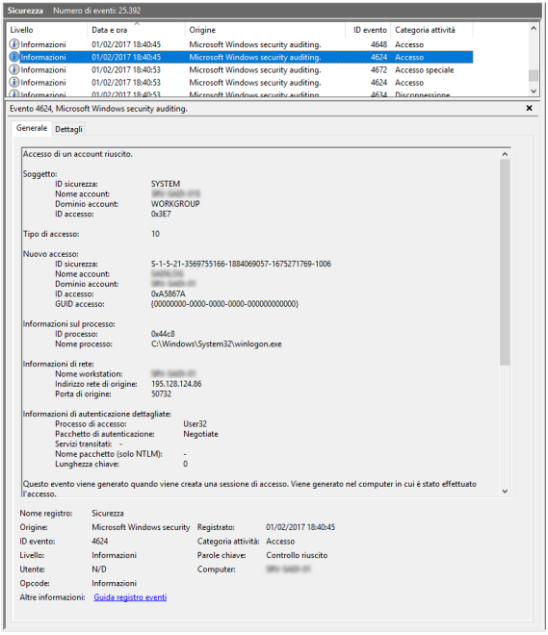
Errori commessi:

- Windows Update disabilitato;
- Desktop remoto aperto esternamente;
- software di assistenza remota come servizio.

In questo caso l'attacco è avvenuto via desktop remoto.







In figura a destra l'accesso alle 18:40 del 01/02/2017 da parte del malfattore (ID evento 4624).

L'accesso è avvenuto dall'IP 195.128.124.86 situato a Mosca in Russia, attraverso le credenziali di un utente non più utilizzato dall'azienda, ma lasciato ancora attivo per collegarsi via desktop remoto.

Famiglie Ransomware

Nel 2016 è stata riscontrato un'esplosione di nuovi crypto-malware e il rilascio di nuove versioni di ransomware sviluppati negli anni precedenti.

Analizziamo ora i crypto-malware più interessanti e che hanno avuto la maggiore diffusione in Italia.

CryptoLocker - TorrentLocker

Anno	2013 settembre
Estensione	.encrypted – .enc - random di 6 caratteri
Algoritmo	AES
Riscatto	100 - 300/600 USD/euro (in Bitcoin/MoneyPak)
Rete	Tor-Onion

Il CryptoLocker è sicuramente il ransomware più noto al mondo, infatti moltissime persone utilizzano il termine "*cryptolocker*" per identificare un qualunque ransomware che cifra i file di documenti o dati.

La prima apparizione di questo crypto-malware risale a settembre del 2013. I file vengono cifrati con l'algoritmo AES aggiungendovi l'estensione ".encrypted". Il CryptoLocker si collega ad una serie di server di C&C per ricevere la chiave di cifratura, in questa fase di scambio con il server di C&C i dati vengono cifrati con RSA.

Le prime versioni del ransomware CryptoLocker creavano la seguente chiave di registro:

```
HKEY_CURRENT_USER\Software\CryptoLocker_####
[PublicKey] = hex:06,02,00,00,00,a4,00,00,52,53,41 [..]
[VersionInfo] = hex:26,30,9c,81,21,b3,3d,d3,ae,33,9c [..]
[WallPaper] = hex:00,00,37,82 [..]
```

dove #### è un numero.

Esempio: `HKEY_CURRENT_USER\Software\CryptoLocker_0388`

Il valore "PublicKey" è una chiave pubblica RSA.

All'interno della chiave "`CryptoLocker_0388`", vi è la sottochiave "`Files`":

`HKEY_CURRENT_USER\Software\CryptoLocker_0388\Files`

dove sono elencati i file cifrati dal ransomware:

[nome file cifrato] = <number dword>

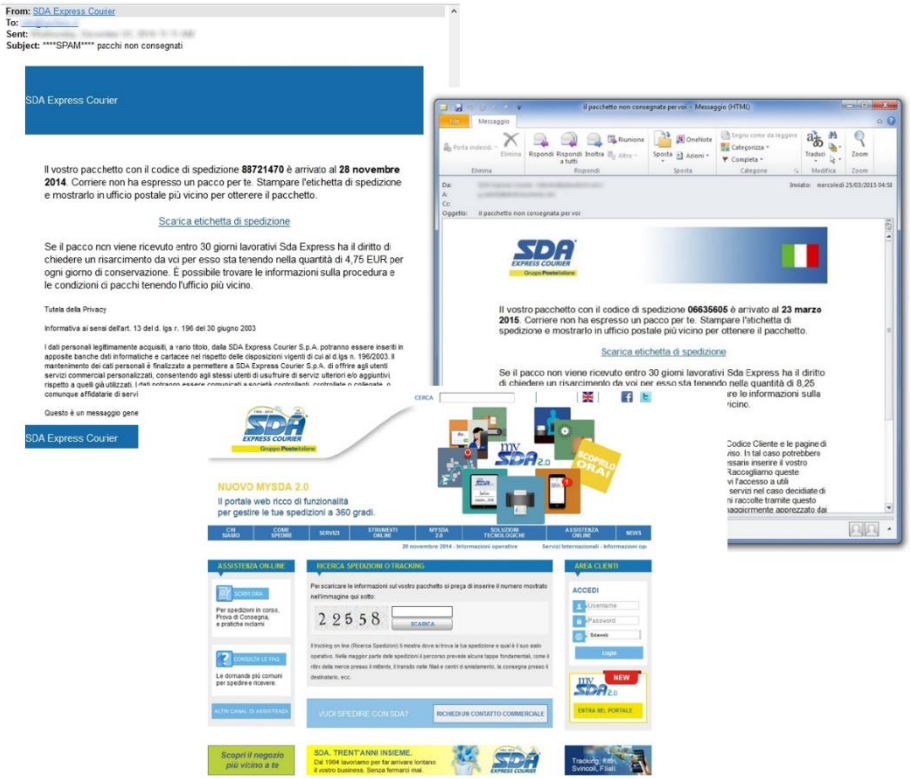
Al termine della cifratura, il CryptoLocker visualizzava le richieste del riscatto:

Nella prima release di settembre 2013 venivano chiesti 100 USD/Euro di riscatto. A partire da dicembre 2013 vengono richiesti 300 USD/Euro in moneta Bitcoin/MoneyPak, che dopo una determinata data raddoppiano a 600.

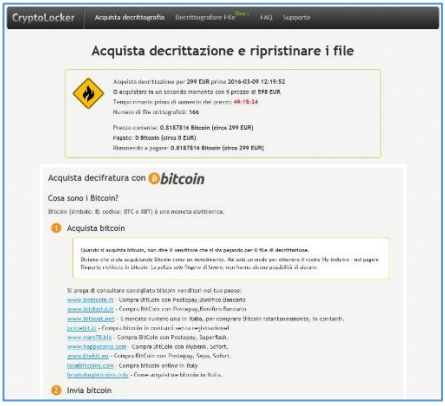
CryptoLocker utilizza la rete Tor-Onion per non essere rintracciato, la moneta richiesta è in BitCoin che permette di avere conti correnti anonimi.

Nel 2014 l'infrastruttura del CryptoLocker è stata smantellata, ma dopo alcuni mesi è stata ricreata sotto il nome di TorrentLocker.

La nuova versione di CryptoLocker (TorrentLocker), a partire dal 2014, ha inviato massive campagne di spam, dove è stata sfruttata l'ingegneria sociale, con finte bollette dell'Enel o di Telecom e di finti pacchi dell'SDA:



Qui possiamo vedere le istruzioni del riscatto della versione TorrentLocker:



E' interessante notare che il CryptoLocker genera un conto corrente (un portafoglio in bitcoin) distinto per ogni vittima dove eseguire il pagamento del riscatto.

Nelle ultime versioni del CryptoLocker, se l'utente era già stato vittima di questo ransomware, il crypto-malware visualizzerà solamente le istruzioni del riscatto e non cifrerà ulteriori file di documento.

CryptoWall

Anno	2014 aprile
Estensione	<casuale>
Algoritmo	RSA-2048
Riscatto	500/1000 USD (in Bitcoin)
Rete	Tor-Onion
Versione	4.0

La prima apparizione di CryptoWall risale ad aprile del 2014. Per la cifratura utilizza l'algoritmo RSA a 2048 bit. I file cifrati, dalla versione 4.0 di Cryptowall hanno nome ed estensione casuale.

Utilizza la rete Tor-Onion e richiede un riscatto iniziale di 500 dollari, che dopo 1 settimana raddoppiano a 1000 dollari (equivalenti in BitCoin).
I vettori di infezioni utilizzati da CryptoWall sono stati l'exploit kit Magnitude nel 2014 e le campagne di spam nel 2015 ("RechnungOnline Monat Februar 2015 (Buchungskonto: 7818210382)", "Incoming Fax Report", etc.).
Istruzioni del riscatto di CrytpoWall 4:

CTB-Locker

Anno	2014 luglio
Estensione	.<casuale di 7 caratteri>
Algoritmo	AES
Riscatto	2 BTC
Rete	Tor-Onion

La prima apparizione di CTB-Locker (Curve Tor Bitcoin Locker) risale a luglio 2014. I file vengono cifrati con l'algoritmo AES e rinominati aggiungendo un'estensione di 7 caratteri casuali. Anch'esso utilizza la rete Tor-Onion e richiede una riscatto di 2 BitCoin che deve essere pagato entro 96 ore.

Istruzioni del riscatto di CTB-Locker:

I vettori di infezioni utilizzati da CTB-Locker sono stati principalmente in Italia campagne di spam.

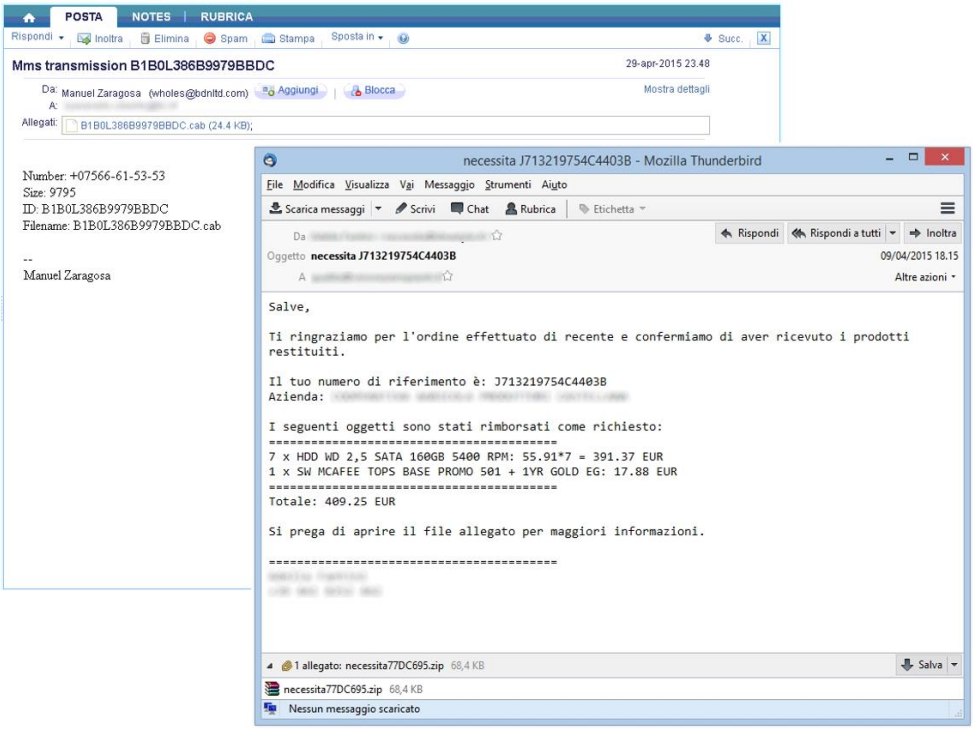
Nel 2015:

- Finti MMS
- Finti ordini di materiale

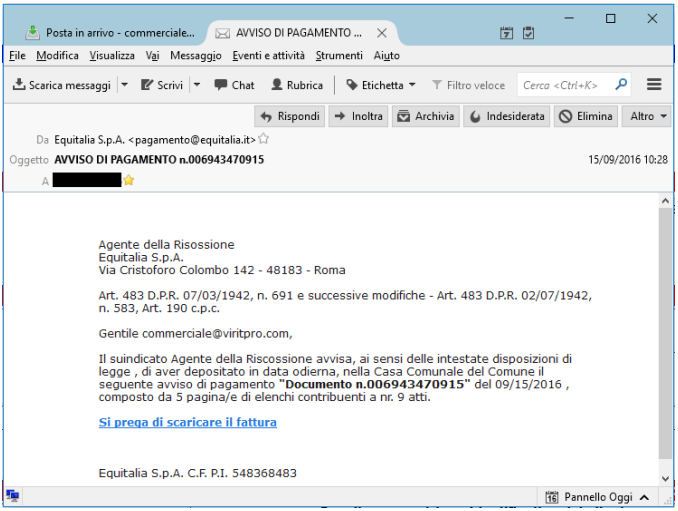
Nel 2016:

- Finti avvisi di Equitalia
- Finte fatture Vodafone
- Finte fatture TIM

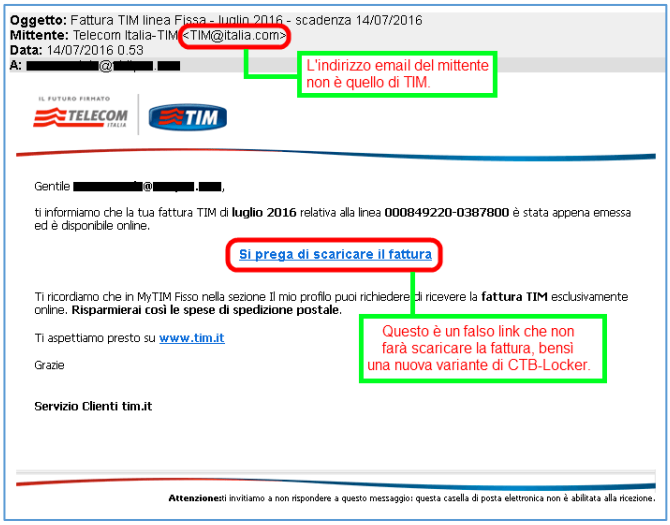
Campagne di CTB-Locker con falso MMS e finto ordine:



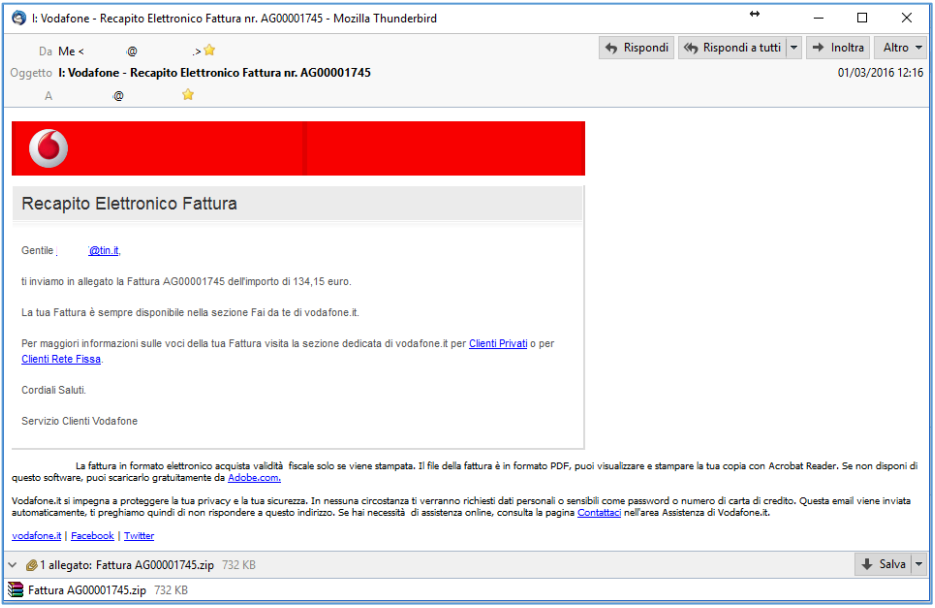
Campagna di Equitalia:



Come si può facilmente notare, vi sono errori ortografici o grammaticali, come “Agente della Risossione” oppure come nell’email della finta fattura TIM:



Per concludere non poteva mancare Vodafone:

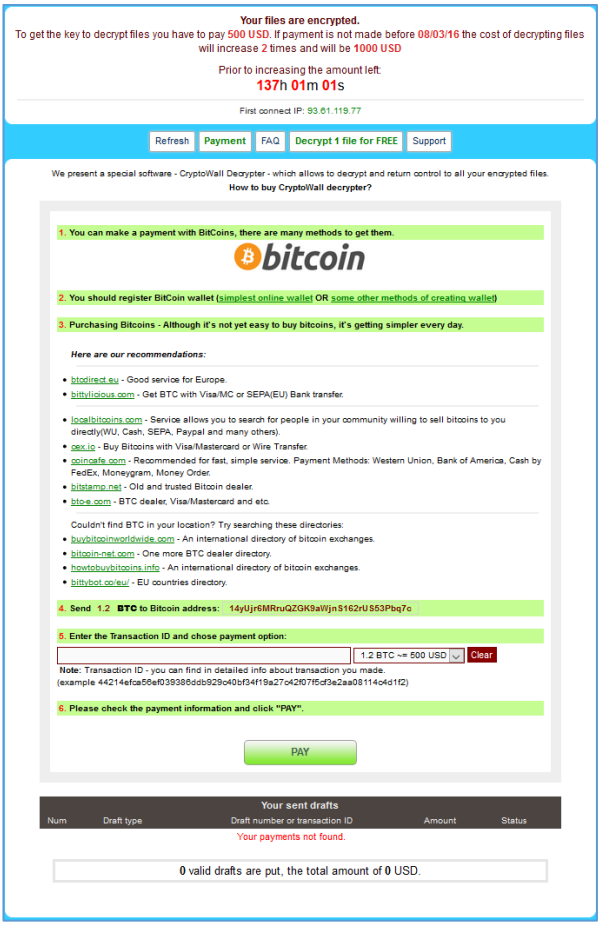


TeslaCrypt

Anno	2015 febbraio
Estensione	.micro, .mp3, .vvv, varie o nessuna estensione
Algoritmo	AES
Riscatto	500/1000 USD (in Bitcoin)
Rete	Tor-Onion
Versione	4.0

La prima apparizione del TeslaCrypt risale a febbraio 2015. I file vengono cifrati con l'algoritmo AES e vengono rinominati con varie estensioni in base alla versione del ransomware. Ad esempio dalla versione 3.0 le estensioni più utilizzate sono state ".micro" e ".mp3".

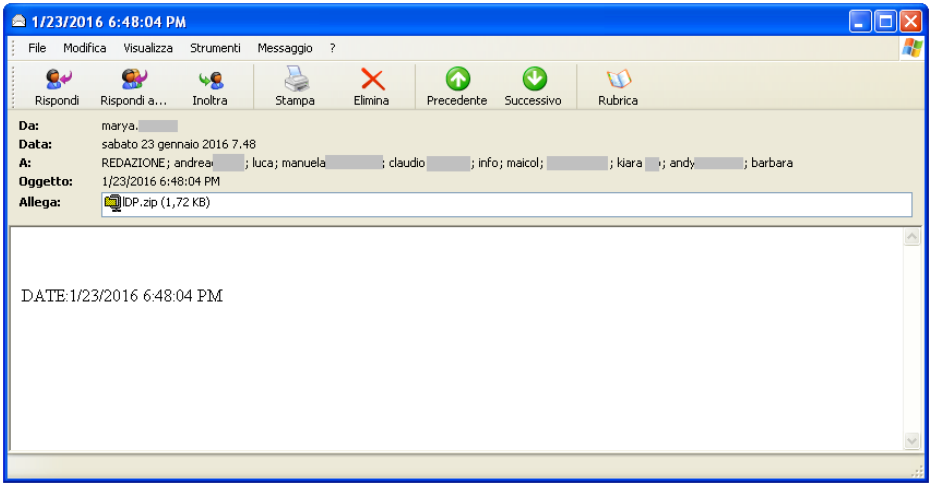
Il TeslaCrypt ha cercato sempre di spacciarsi per altri ransomware, visualizzando le medesime richieste di riscatto, come possiamo vedere qui che si spaccia da CryptoWall.



Il riscatto richiesto è di 500 dollari, che dopo 1 settimana raddoppia a 1000.

I vettori di infezione maggiormente utilizzati sono stati gli exploit kit, come Neutrino e Angler, ma anche attraverso il canale della posta elettronica.

Tra la fine di gennaio e l'inizio di febbraio 2016 vi è stato un massivo invio di email (più di 45 milioni) infette da TeslaCrypt:



Il 1° febbraio 2016 si è riscontrato il picco dell'infezioni da ransomware di tutto il 2016 generate da TeslaCrypt.

Il ransomware TeslaCrypt è diventato nel giro di pochi mesi uno dei più temibili crypto-malware in circolazione. TeslaCrypt nasce a febbraio 2015, fino alla versione 2.0 (dicembre 2015) di questo ransomware era possibile decifrare i file criptati. Il punto di svolta di TeslaCrypt è avvenuto a gennaio 2016, quando verso metà mese fu rilasciata la versione 3.0. Tale versione era impossibile da decifrare, tutti gli errori commessi nelle precedenti versioni erano state corretti e l'utilizzo dell'algoritmo AES a 256 bit rendeva impossibile decifrare i file.

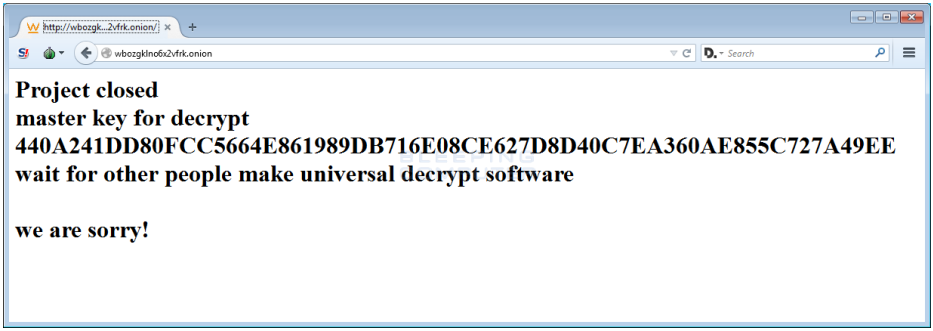
Gli attacchi del 1° e del 22 febbraio di TeslaCrypt 3.0 avevano mietuto moltissime vittime in tutto il mondo. Ma qualcosa stava cambiando tra gli autori di TeslaCrypt, infatti a marzo 2016 in modo inaspettato viene rilasciata la versione 4.0. Una versione 4.0 che non andava a correggere punti deboli della versione 3.0, ma avevano come riscritto il codice utilizzando differenti librerie per implementare l'algoritmo AES di cifratura.

La struttura concettuale del malware era la stessa, ma avevano come "ripulito" il codice della versione 3.0.

Questo cambiamento repentino, ha fatto pensare ai ricercatori anti-virus, che gli autori stessero vendendo il progetto TeslaCrypt a qualcun altro, come un servizio RaaS (Ransomware as a Service).

La versione 4.0 di TeslaCrypt è stata diffusa fino ad aprile 2016.

A maggio 2016 è avvenuta una cosa sorprendente, un ricercatore di Eset si era accorto che da alcune settimane non vi erano più infezioni di TeslaCrypt. Ha contattato gli autori di TeslaCrypt attraverso il loro sito di Tor-Onion chiedendo delucidazioni sull'accaduto e la risposta degli autori di TeslaCrypt fu che avevano chiuso il progetto. Dopo alcuni giorni gli stessi autori del ransomware hanno rilasciato la chiave Master Key con cui si poteva decifrare qualsiasi versione di TeslaCrypt:



Rimane ancora un mistero il motivo del rilascio della chiave di cifratura Master Key da parte degli autori di TeslaCrypt.

Nel prosieguo torneremo ancora sul caso TeslaCrypt.

Locky (Zepto, Odin, Thor, Osiris)

Anno	2016 febbraio
Estensione	.locky, .zepto, .odin, .sh*t, .thor, .osiris, etc
Algoritmo	RSA – AES
Riscatto	0,5 -1 – 3 BTC (in base alla versione)
Rete	Tor-Onion

Il ransomware Locky fa la sua prima apparizione a febbraio del 2016. Locky utilizza l'algoritmo AES per cifrare i file e RSA per scambiare la chiave di cifratura con il server di comando e controllo. Nelle prime versioni aggiungeva l'estensione ".locky" ai file cifrati. A giugno viene rilasciata una nuova release che cifrava i file aggiungendo l'estensione ".zepto". A settembre 2016 i file cifrati vengono rinominati in ".odin". A ottobre l'autore di Locky rilascia 2 nuove release che rinominano i file in ".sh*t" e ".thor". A dicembre viene rilasciata la release che rinomina i file in ".osiris".

In pochi mesi è diventato lo "spauracchio" degli ospedali americani, molte sono state le strutture mediche colpite dal ransomware Locky, come l'Hollywood Presbyterian Medical Center in Los Angeles a febbraio 2016 e il Methodist Hospital in Henderson (Kentucky) a marzo 2016.

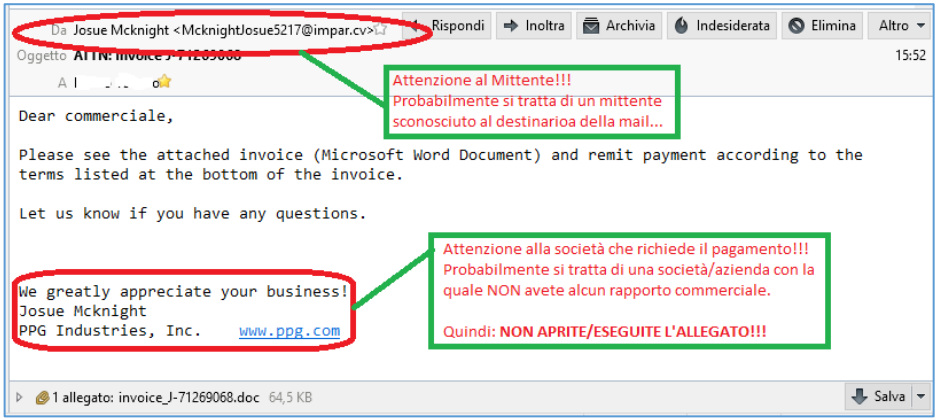
Secondo Allen Stefanek, presidente e CEO dell'Hollywood Presbyterian Medical Center, come riportato in un documento ufficiale, il riscatto pagato è stato di 40 Bitcoin circa 17000 dollari.

I vettori di infezione utilizzati da Locky sono l'invio di campagne di spam, contenenti documenti di Word con macro infette oppure file .zip contenenti Javascript, e attraverso gli exploit kit come Neutrino, Nuclear Pack e Rig EK.

Esempi di campagne:

Oggetto	Allegato
ATTN: invoice_J-71269068	invoice_ J-71269068.doc
Delay with Your Order #1629ADCD, Invoice #44196947	order_copy_1629ADCD.zip
Emailing: MX62EDO 01.03.2016	MX62EDO201603016735093.zip
Updated	<nome>_updated_doc_<numero>.zip
Scanned image	<data>_<numeri casuali>.docm

Ad esempio nella prima versione di Locky a febbraio 2016, si trasmetteva via email allegando il documento "**invoice_<stringa casuale>.doc**".



L'apertura del documento di Word, comportava l'esecuzione di una macro che andava a scaricare ed eseguire un file eseguibile con nome casuale contenente il Locky.

Il file eseguibile con nome casuale, si copiava nella cartella %temp% dell'utente con nome SVCHOST.EXE.

A questo punto Locky esegue la cancellazione delle "shadow copy" con il comando: **vssadmin.exe Delete Shadows /All /Quiet**

Esegue una serie di thread in parallelo per la cifratura dei documenti (nella nostra macchina di test ne aveva eseguiti 13). Il malware Locky cripta ogni file con le seguenti estensioni:

.m4u .m3u .mid .wma .flv .3g2 .mkv .3gp .mp4 .mov .avi .asf .mpeg .vob .mpg .wmv .fla .swf .wav .mp3 .qcow2 .vdi .vmdk .vmx .gpg .aes .ARC .PAQ .tar .bz2 .tbk .bak .tar .tgz .gz .7z .rar .zip .djv .djvu .svg .bmp .png .gif .raw .cgm .jpeg .jpg .tif .tiff .NEF .psd .cmd .bat .sh .class .jar .java .rb .asp .cs .brd .sch .dch .dip .pl .vbs .vb .js .h .asm .pas .cpp .c .php .ldf .mdf .ibd .MYI .MYD .frm .odb .dbf .db .mdb .sql .SQLITEDB .SQLITE3 .asc .lay6 .lay .ms11 (Security copy) .ms11 .sldm .sldx .ppsm .ppsx .ppam .docb .mml .sxm .otg .odg .uop .potx .potm .pptx .pptm .std .sxd .pot .pps .sti .sxi .otp .odp .wb2 .123 .wks .wk1 .xltx .xltm .xlsx .xlsm .xlsb .slk .xlw .xlt .xlm .xlc .dif .stc .sxc .ots .ods .hwp .602 .dotm .dotx .docm .docx .DOT .3dm .max .3ds .xml .txt .CSV .uot .RTF .pdf .XLS .PPT .stw .sxw .ott .odt .DOC .pem .p12 .csr .crt .key wallet.dat

Il Locky cifra tutti i documenti rinominandoli con nome casuale e estensione .Locky. I file con estensione .Locky avranno nome `<ID><casuale>.locky` (esempio: 1DD6FF20B0293D341C12403B3C699ADF.locky)

I file di documenti originali verranno dopo completamente sovrascritti con il carattere "U" e cancellati. Il malware modifica le seguenti chiavi di registro per mettersi in esecuzione automatica:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Run\Locky] = %temp%\svchost.exe
```

Terminata la cifratura dei file Locky crea il file *_Locky_recover_instructions.txt* contenente le istruzioni per il riscatto e modifica l'immagine del desktop in *_Locky_recover_instructions.bmp*.

Inoltre crea la chiave di registro:

HKEY_CURRENT_USER\Software\Locky	
[id]	id della vittima
[pubkey]	chiave pubblica RSA
[paytext]	informazioni del riscatto
[completed]	se vale 1 allora ha completato la cifratura dei file

Al termine il Locky modifica la chiave di registro "*pending rename file*" per cancellarsi al successivo riavvio del computer, lasciando solamente le istruzioni per il riscatto.

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://6dtxgqam4crv6rr6.tor2web.org/782EF05A6522940A
2. http://6dtxgqam4crv6rr6.onion.to/782EF05A6522940A
3. http://6dtxgqam4crv6rr6.onion.cab/782EF05A6522940A
4. http://6dtxgqam4crv6rr6.onion.link/782EF05A6522940A

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dtxgqam4crv6rr6.onion/782EF05A6522940A
4. Follow the instructions on the site.

!!! Your personal identification ID: 782EF05A6522940A !!!

Locky Decryptor™

We present a special software - Locky Decryptor™ -
which allows to decrypt and return control to all your encrypted files.

How to buy Locky Decryptor™?

1 You can make a payment with BitCoins, there are many methods to get them.

2 You should register BitCoin wallet:

Simplest online wallet or Some other methods of creating wallet

3 Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

localbitcoins.com (WU)	Buy Bitcoins with Western Union.
coincafe.com	Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
localbitcoins.com	Service allows you to search for people in your community willing to sell bitcoins to you directly.
cex.io	Buy Bitcoins with VISA/MASTERCARD or wire transfer.
btcdirect.eu	The best for Europe.
bitquick.co	Buy Bitcoins instantly for cash.
howtobuybitcoins.info	An international directory of bitcoin exchanges.
cashintocoins.com	Bitcoin for cash.
coinjar.com	CoinJar allows direct bitcoin purchases on their site.
anxpro.com	
bittylicious.com	

4 Send 3.00 BTC to Bitcoin address:

1A93caMDS6XnNMTmaf3CXfsBp3whFFBnp8

Note: Payment pending up to 30 mins or more for transaction confirmation, please be patient...

Date	Amount BTC	Transaction ID	Confirmations
not found			

5 Refresh the page and download decryptor.

When Bitcoin transactions will receive one confirmation, you will be redirected to the page for downloading the decryptor.

Cerber

Anno	2016 marzo
Estensione	.cerber(2)(3), casuale di 4 caratteri
Algoritmo	RSA - AES
Riscatto	1 – 2 - 2,4 BTC (in base alla versione)
Rete	Tor-Onion
Diffusione	siti compromessi, HydraBot, in bundle con Ammyy, mail

A marzo 2016 si diffonde il ransomware Cerber attraverso siti compromessi dall'exploit kit Neutrino. Cerber utilizza l'algoritmo AES per cifrare i file e la chiave viene cifrata con RSA durante la fase di comunicazione con il server di C&C.

I file cifrati hanno nome casuale e estensione ".cerber" (es. 6CA_vCkMYg.cerber). Nelle versione successive l'estensione sono divenute in base alla versione del malware in .cerber2, .cerber3 e casuale.

Nella prima versione di marzo 2016 del Cerber, il file portatore veniva spostato dalla cartella %appdata% dell'utente con nome *makecab.exe* Questo file era messo in esecuzione automatica in vari modi:

```
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion
\Run]

makecab = %appdata%\Roaming\{2FC5AFB6-1BDA-FA2C-4A7C-
3BC9BCCA37EE}\makecab.exe

[HKEY_CURRENT_USER\Control Panel\Desktop]

SCRNSAVE.EXE = %appdata%\Roaming\{2FC5AFB6-1BDA-FA2C-4A7C-
3BC9BCCA37EE}\makecab.exe

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Command Processor]

AutoRun = %appdata%\Roaming\{2FC5AFB6-1BDA-FA2C-4A7C-
3BC9BCCA37EE}\makecab.exe
```

Al termine della cifratura vengono rilasciate le istruzione del riscatto nei file "**# DECRYPT MY FILES #.html**" e "**# DECRYPT MY FILES #.txt**":

C E R B E R

Your documents, photos, databases and other important files have been encrypted!
To decrypt your files you need to buy the special software – "Cerber Decryptor".
For more specific instructions, please visit your personal home page, there are a few
different addresses pointing to your page below:

---

1. http://decrypttozxybarc.dconnect.eu/54A0-7C12-B1E9-004E-XXXX
2. http://decrypttozxybarc.tor2web.org/54A0-7C12-B1E9-004E-XXXX
3. http://decrypttozxybarc.onion.cab/54A0-7C12-B1E9-004E-XXXX
4. http://decrypttozxybarc.onion.to/54A0-7C12-B1E9-004E-XXXX
5. http://decrypttozxybarc.onion.link/54A0-7C12-B1E9-004E-XXXX

If for some reasons the addresses are not available, follow these steps:

---

1. Download and install the "Tor Browser" from https://www.torproject.org/
2. Run it
3. In the "Tor Browser" open website:
http://decrypttozxybarc.onion/54A0-7C12-B1E9-004E-XXXX
4. Follow the instructions at this website

"...Quod me non necat me fortiorem facit."

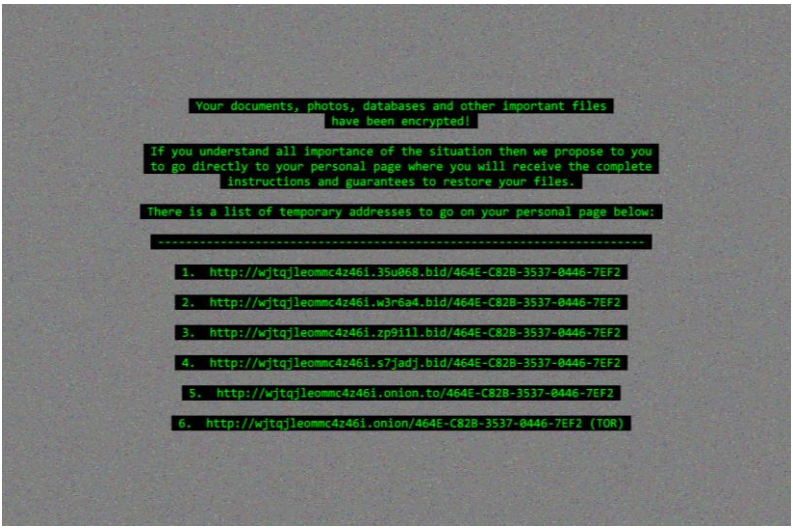
Da notare la frase in latino lasciata dagli autori del crypto-malware di cattivo presagio: "***...Quod me non necat me fortiorem facit***" (ciò che non mi uccide, mi rende più forte).

Inoltre il Cerber crea il seguente file "**# DECRYPT MY FILES #.vbs**" in VBScript:

```
1  Set SAPI = CreateObject("SAPI.SpVoice")
2  SAPI.Speak "Attention! Attention! Attention!"
3  For i = 1 to 7
4  SAPI.Speak "Your documents, photos, databases and other important files have been encrypted!"
5  Next
```

Lo script permette al Cerber di parlare alla sua vittima, dicendo: "*Your documents, photos, databases and other important files have been encrypted!*".

Nelle versioni successive del Cerber, il ransomware modificava lo sfondo del desktop con la richiesta del riscatto, come possiamo vedere nella versione 3:

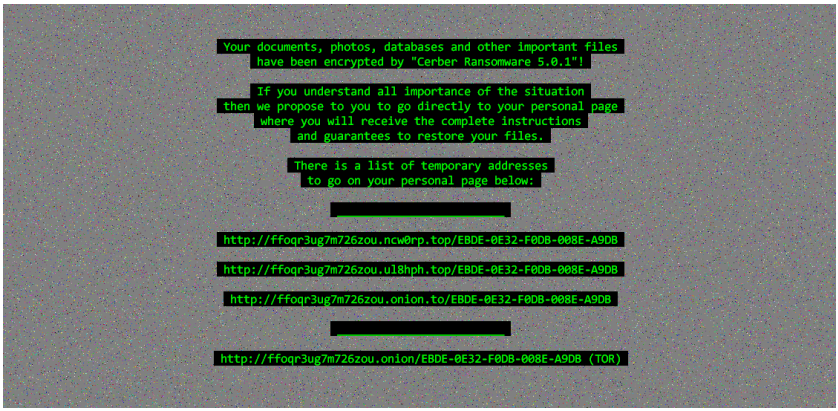


Negli ultimi mesi il Cerber ha avuto diverse evoluzioni, ad esempio ad agosto 2016 è passato dalla versione 2 alla versione 3 nello stesso mese. All'inizio del mese di agosto era stata rilasciata la versione 2 del Cerber, e a metà agosto i ricercatori di CheckPoint avevano notato una falla nel sistema di comunicazione con il server di comando e controllo, che permetteva di decifrare i file di documento. Qualche giorno dopo, la vulnerabilità è stata corretta con il rilascio di Cerber 3.

Gli autori di Cerber hanno iniziato a rendersi ostili alle tecnologie anti-ransomware, adottando nuove tecniche per eludere questi sistemi di protezione come in una partita a scacchi. Dalla versione 3 di Cerber, i file venivano cifrati a partire dall'offset 512 e non dall'inizio dei file come nelle versioni precedenti.

A ottobre 2016 è stata rilasciata la versione 4 di Cerber, a partire da questa release nella schermata con le istruzioni del riscatto viene indicata anche la versione del ransomware Cerber.

A fine novembre viene rilasciata la versione 5 il cui offset di inizio cifratura è stato spostato al valore 640.



A dicembre 2016 viene diffusa una nuova release di Cerber nota con il nome ***Cerber Red*** che sembra essere una versione modificata del Cerber 3, infatti l'offset di inizio cifratura è tornato al valore 512, qui possiamo vedere la sua richiesta di riscatto:

Il ransomware Cerber utilizza diversi vettori di infezioni: exploit kit, attraverso altri malware come HydraBot, in bundle con altri software legittimi e campagne di spam.

Interessante è il caso di Ammyy a metà settembre del 2016, che distribuiva il ransomware Cerber. A partire dal 18 settembre scaricando dal sito ufficiale la versione del software di assistenza remota AMMYY, procedendo all'installazione, si attiva il temibile ransomware Cerber nella sua versione 3.

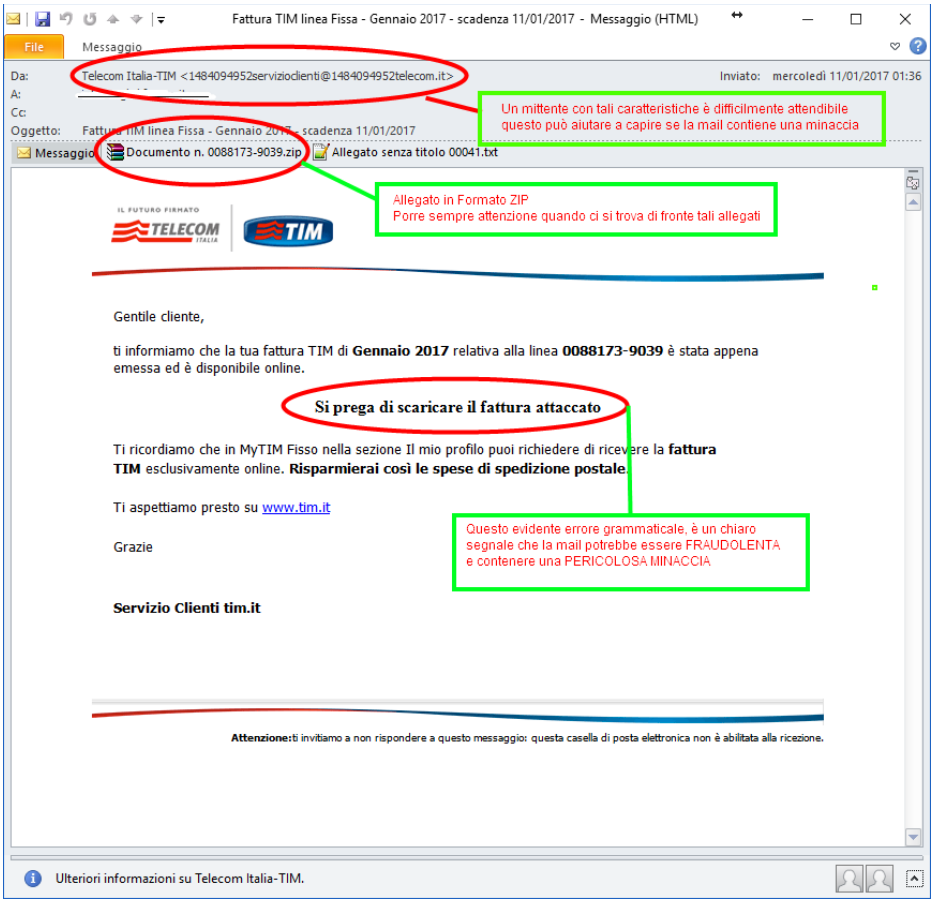
Eseguendo il file di installazione scaricato dal sito ufficiale di AMMYY, come detto, si attivava in prima battuta il processo **ENCRYPTED.EXE** contenente il Cerber 3, che andava a cifrare i file di dati del PC / SERVER e delle unità mappate di rete. Di fatto contemporaneamente veniva estratto/copiato il file di installazione originale di AMMYY.

Una versione di AMMYY del 20 settembre 2016 taroccata con il Cerber:

Nome File	AA_v3.5.exe
Dimensione	1303197 byte
MD5	300e85c8ab120c432cf81aeafbefb090
Data di compilazione	19/06/1992 22.22.17
Firma digitale	-
Commento	Il file infetto contiene il ransomware **Cerber 3** nel file **Encrypted.exe** (dimensione 331966 byte, MD5 20bfaa96d3560dc255a5766c12350367, data compilazione 19/09/2016 19.59.29), e il file originale di Ammy v. 3.5

Le versioni infette di AMMYY si sono susseguite anche nei giorni successivi.

Per quanto riguarda le campagne di spam, ultimamente, questo vettore di infezione è utilizzato dalla versione Cerber Red, che si sta diffondendo con false mail di fatture Telecom-TIM e Vodafone:



Petya

Anno	2016 marzo
Tipo	Cifra la Master File Table
Algoritmo	Salsa20
Riscatto	0,99 BTC
Rete	Tor-Onion
Versione	4.0 Goldeneye

Petya è stato scoperto a marzo del 2016, ed è salito alla ribalta perché si differenzia dagli altri ransomware andando a cifrare la Master File Table invece dei file di documento, rendendo impossibile l'accesso ai file.

L'algoritmo di cifratura utilizzato è Salsa20, utilizza la rete Tor-Onion e richiede un riscatto di circa un 1 BTC.

Vi sono 4 versioni di Petya:

- Petya.A (red version – marzo 2016)
- Petya.B (green version – maggio 2016)
- Petya.C (green version - luglio 2016)
- Petya.D (yellow version – dicembre 2016)

Il ransomware Petya si è diffuso massivamente attraverso campagne di spam in Germania. La prima mail infetta, naturalmente scritta in lingua tedesca, invitava a scaricare da un cartella di Dropbox due documenti:

- Bewerbungspoto.jpg
- Bewerbungsmappe-gepackt.exe

L'esecuzione del file eseguibile Bewerbungsmappe-gepackt.exe con i diritti di Administrator, contenente il dropper di Petya, comportava la sovrascrittura del MBR (Master Boot Record) e il blocco del computer con la visualizzazione di una schermata BSOD (Blue Screen of Death). Al

successivo riavvio veniva visualizzato una finta schermata di chkdsk, che in realtà va a cifrare la Master File Table.

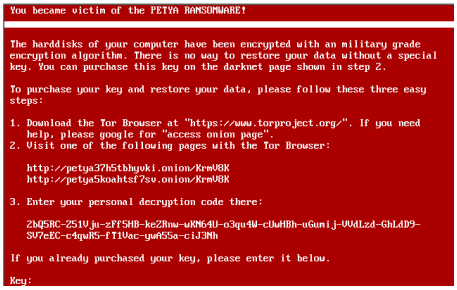
```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 6506 of 43712 (14%)
```

Al termine del finto “chkdsk”, il computer si riavvia automaticamente visualizzando cosa effettivamente era successo:



Una prima schermata visualizza il teschio della morte, premendo un tasto, segue la schermata con le richieste di riscatto Petya.

Petya.A: attacco (fase 1)

Nome	Bewerbungsmappe-gepackt.exe
MD5	af2379cc4d607a45ac44d62135fb7015
Dimensione	230912 byte

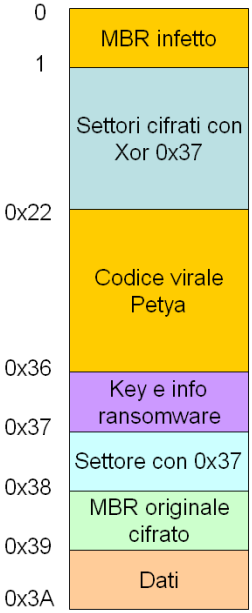
Questa release di Petya necessitava di essere eseguita con i privilegi di Administrator.

L'esecuzione del dropper di Petya contenuto in Bewerbungsmappe-gepackt.exe, portava il computer in blocco, visualizzando la schermata di BSOD (Blue Screen of Death) riportata qui a fianco.

La schermata BSOD visualizzava un messaggio di errore in lingua italiana, molto probabilmente dovuto alla versione in italiano di Windows.
A questo punto il malware ha infettato l'MBR (Master Boot Record) del disco fisso e ha sovrascritto alcuni settori compresi tra l'MBR e il Boot Sector della partizione. In questa fase non ha ancora iniziato a cifrare l'MFT (Master File Table).

Disco infetto dopo l'esecuzione del dropper del Petya:

Il settore 0 dell'MBR è infettato dal codice di loader del Petya. La lunghezza di questo codice è di 147 byte.
I settori dall'1 al 0x21 sono cifrati con XOR 0x37.
Dal settore 0x22 al 0x35 troviamo il codice virale di Petya Ransomware.
Nel settore 0x36 vi troviamo la key utilizzata per la cifratura, un vettore, gli indirizzi Tor-Onion e l'ID della vittima.
Il settore 0x37 è utilizzato per la verifica della key, in questa fase ogni byte del settore contiene il valore 0x37.
Nel settore 0x38 vi troviamo l'MBR originale cifrato con XOR 0x37.
Il settore 0x39 è vuoto, contiene solo zeri.

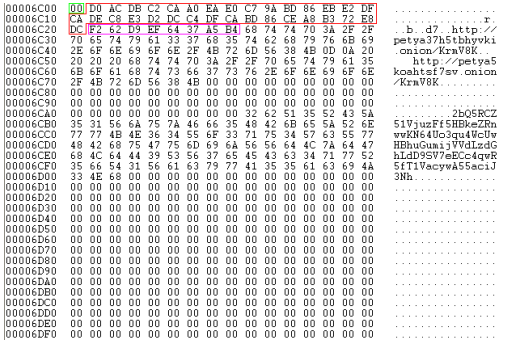


Analizziamo in modo più dettagliato il settore 0x36:

off 0x0: 1 byte: valore che indica lo stato del disco

- 0: disco da cifrare
- 1: disco cifrato
- 2: disco de-cifrato

off 0x01: (32 byte) key utilizzata per la cifratura
off 0x21: (8 byte) vettore utilizzato per la cifratura
off 0x29: (128 byte) indirizzi Tor-Onion per pagare il riscatto
off 0xa9: (90 byte) id vittima



In questo momento il disco o meglio la MFT (Master File Table) non è ancora stata cifrata. Se il computer viene spento e riavviato da un cd bootable oppure collegato l'hard disk come secondario ad un altro pc, è possibile rimuovere l'infezione con il comando FIXMBR senza perdere nessun dato.

Se invece il computer viene riavviato o acceso, il codice virale del Petya andrà a cifrare la Master File Table.

Petya.A: il primo boot (fase 2)

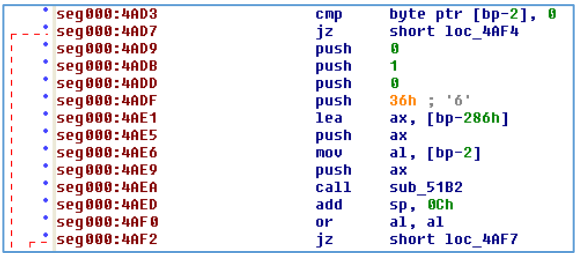
Vediamo ora che cosa avviene quando viene eseguito per la prima volta (il primo boot) l'MBR infetto da Petya.

Quando viene accesso il computer, il Bios andrà ad eseguire il codice contenuto nel settore 0 (MBR) del disco. Il codice dell'MBR viene caricato al seguente indirizzo: 0:7c00. L'MBR infetto da Petya va a leggere 0x20 settori partendo dal settore 0x22 e li carica all'indirizzo: 0:8000, dove salta a quell'indirizzo con un JMP.

Ora all'indirizzo 0:8000 avremo tutto il codice del Petya attivo in memoria.

La prima operazione che fa è quella di leggere le partizioni di tutti di dischi collegati e di memorizzarli in una tabella.

A questo punto va leggere il settore 0x36 in memoria:



```
seg000:4AD3          cmp     byte ptr [bp-2], 0
seg000:4AD7          jz      short loc_4AF4
seg000:4AD9          push    0
seg000:4ADB          push    1
seg000:4ADD          push    0
seg000:4ADF          push    36h ; '6'
seg000:4AE1          lea     ax, [bp-286h]
seg000:4AE5          push    ax
seg000:4AE6          mov     al, [bp-2]
seg000:4AE9          push    ax
seg000:4AEA          call    sub_51B2
seg000:4AED          add     sp, 0Ch
seg000:4AF0          or      al, al
seg000:4AF2          jz      short loc_4AF7
```

La funzione "sub_51b2" è utilizzata per leggere o scrivere settori del disco.

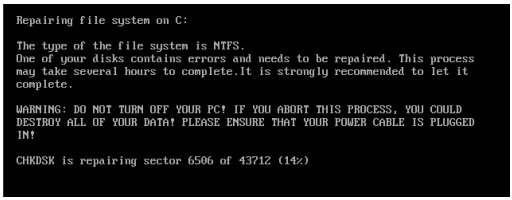
Prototipo: (drive, indirizzo del buffer, (DWORD) settore assoluto, num. di settori, 0/1)

L'ultimo parametro indica la lettura (0) o la scrittura (1).

A questo punto verifica il valore del primo byte del settore 0x36, cioè quella del campo "stato del disco". Se vale 0 inizierà la procedura di cifratura, altrimenti visualizzerà le istruzioni del riscatto.

Essendo il primo boot, il codice virale troverà il valore 0, che indica che il Petya deve cifrare la Master File Table.

A questo punto inizia la fase di cifratura, con la visualizzazione dei messaggi del falso chkdsk.



```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 6506 of 43712 (14%)
```

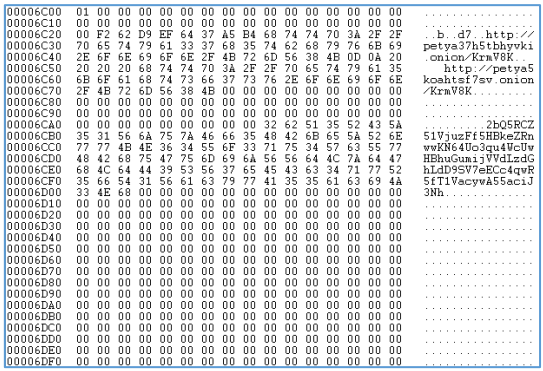
Vediamo più in dettaglio questa fase di cifratura:

Step 1: lettura della key in memoria e sua cancellazione dal disco

1. Petya legge nuovamente il settore 0x36 in memoria
2. Imposta a 1 il valore del primo byte del settore 0x36 caricato in memoria (stato del disco)
3. Copia la key da 32 byte in un buffer interno e azzera quella in memoria del settore 0x36
4. Riscrive il settore 0x36 modificato

Settore 0x36 modificato ->

A questo punto la key a 32 byte per la cifratura è presente solo in memoria.



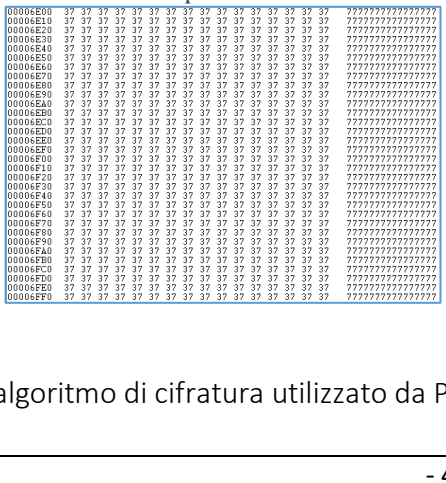
Step 2: cifratura del settore 0x37

Ora Petya va a cifrare il settore 0x37 (che conteneva tutti i byte di valore 0x37) con la key a 32 byte (residente in memoria)

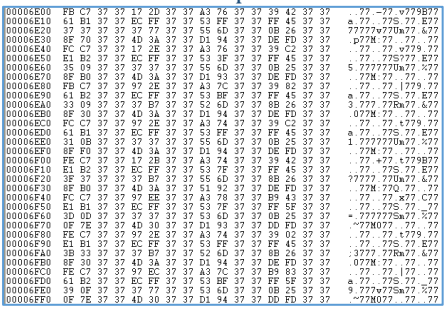
- Lettura del settore 0x37 in memoria
- Cifratura del buffer in memoria del settore 0x37 con la key a 32 byte e il vettore a 8 byte (settore 0x36)
- Scrittura del settore 0x37 cifrato

La cifratura del settore 0x37 permette a Petya di verificare se la chiave inserita è corretta.

Settore 0x37: prima della cifratura



Settore 0x37: dopo la cifratura



L'algoritmo di cifratura utilizzato da Petya.A è Salsa20.

E' necessario preparare una "master table" di 64 byte:

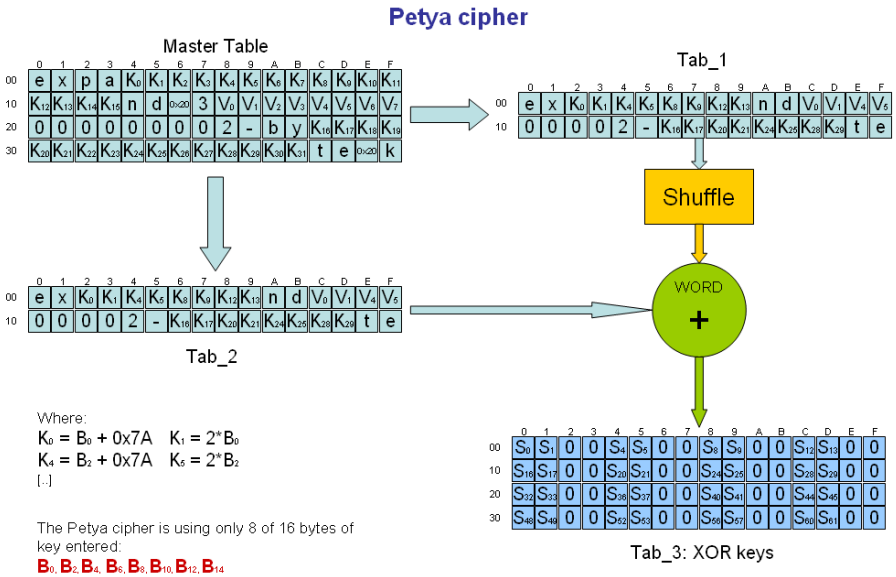
- "expand 32-byte k"
- Key da 32 byte
- Vettore di inizializzazione da 8 byte (settore 0x36)
- Contatore da 8 byte (valore iniziale 0)

Master Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	e	x	p	a	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
10	K_{12}	K_{13}	K_{14}	K_{15}	n	d	0x20	3	V_0	V_1	V_2	V_3	V_4	V_5	V_6	V_7
20	0	0	0	0	0	0	0	2	-	b	y	K_{16}	K_{17}	K_{18}	K_{19}	
30	K_{20}	K_{21}	K_{22}	K_{23}	K_{24}	K_{25}	K_{26}	K_{27}	K_{28}	K_{29}	K_{30}	K_{31}	t	e	0x20	k

Salsa20 è un algoritmo di cifratura che esegue operazioni a 32 bit (add, xor, rot). La versione di Salsa20 implementata in Petya.A esegue operazioni a 16 bit !!!

Qui possiamo vedere lo schema di cifratura utilizzato da Petya applicando l'algoritmo di cifratura Salsa20 con operazioni a 16 bit, nella scatola denominata "shuffle" vengono eseguite le operazioni di "scramble" come *add*, *xor* e *rot*. La tabella di output ottenuta è di 64 byte ed è utilizzata per eseguire la cifratura attraverso l'operatore XOR:



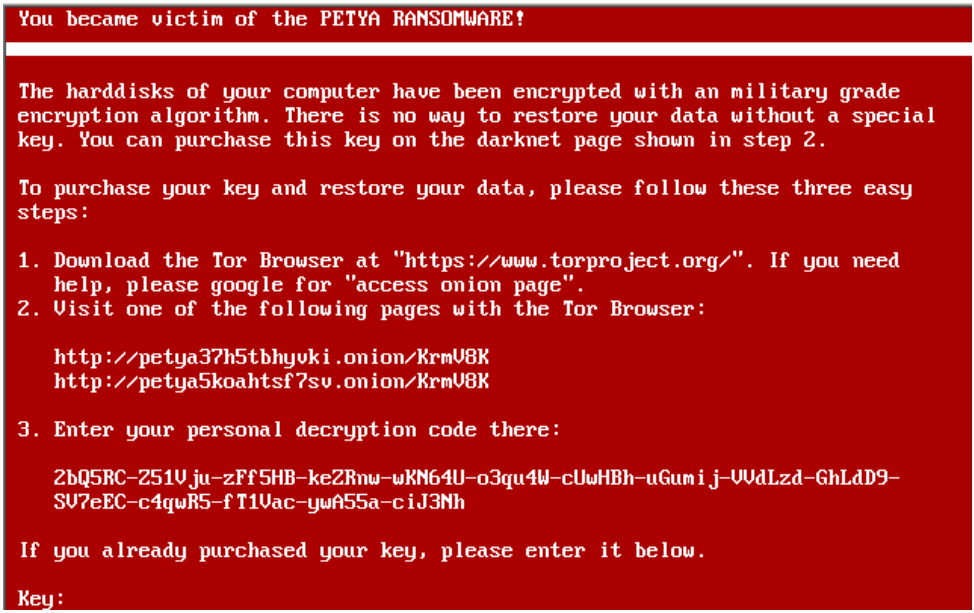
Step 3: Cifratura della Master File Table

1. Scrittura del settore 0x39 con tutti zeri (lo ripete su tutti i dischi collegati)
2. Lettura del Boot Sector
3. Calcola la posizione dell'MFT sul disco
4. Legge 2 settori dell'MFT
5. Dal record con attributo 0x80 determina il numero totale di settori da cifrare e il settore assoluto da cui iniziare
6. Cifratura dei settori dell'MFT con la key a 32 byte e il vettore a 8 byte (vengono cifrati 8 settori alla volta fino al raggiungimento del numero prestabilito)
7. Scrittura del settore 0x39 con il numero totale dei cluster cifrati
8. Riavvio del computer

A questo punto Petya ha cifrato la Master File Table e al successivo riavvio verranno visualizzate le istruzioni del riscatto.

Petya.A: verifica della key (fase 3)

Ai successivi boot, dopo la visualizzazione del teschio della morte, Petya avverte l'utente che è vittima di un ransomware e rimane in attesa dell'inserimento della key acquista.



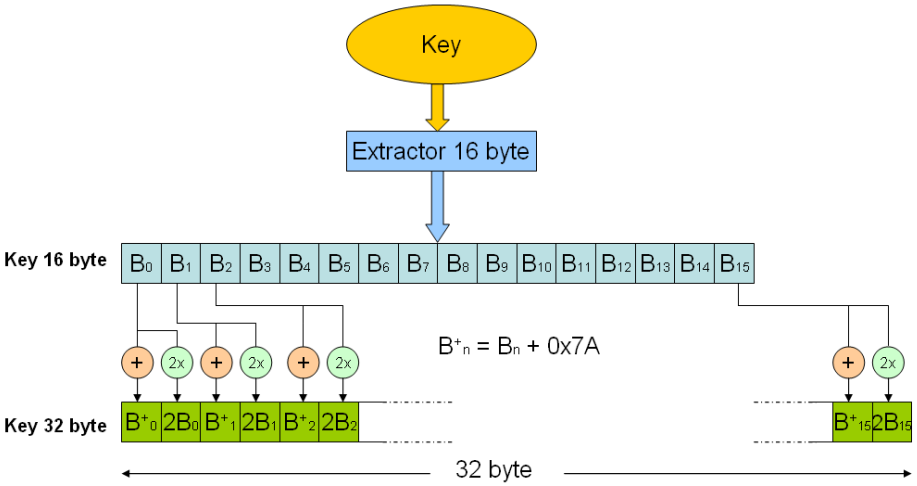
Vediamo ora la verifica della key inserita, in che modo Petya verifica se la chiave corretta è quella esatta.

La lunghezza della key inserita deve essere compresa tra 16 e 73 caratteri. Solo i caratteri compresi tra lo spazio ' ' asc(0x20) e la '~' asc (0x7e) saranno stampati a video.

Dalla key inserita vengono presi i primi 16 caratteri appartenenti al seguente insieme:

123456789abcdefghijkmnopqrstuvwxABCDEFGHJKLMNPQRSTUVWX

Dalla Key da 16 byte si ottiene una Key da 32 byte come rappresentato in figura:



La Key da 32 byte sarà utilizzata per decifrare da Petya.

Ottenuta la Key da 32 byte, Petya esegue le seguente operazioni:

1. Lettura del settore 0x36 per leggere il vettore da 8 byte
2. Lettura del settore 0x37
3. Tramite la Key da 32 byte ottenuta e il vettore da 8 byte decifra il settore 0x37, se ogni byte del settore 0x37 ha valore 0x37 allora la key è esatta, nel caso contrario visualizza messaggio di "Invalid key!"
4. Se la chiave è esatta, pone a 2 il primo byte del settore 0x36 e scrive la key da 32 byte nel medesimo settore.
5. Decifra il master File Table (MFT)
6. Legge il settore 0x38 dove è memorizzato l'MBR cifrato con XOR 0x37, dopo averlo decifrato lo scrive nel settore 0.
7. Decifra i settori da 0x1 a 0x21 che erano cifrati con XOR 0x37
8. In casi particolari (se all'offset 0 x1b8 dell'MBR contiene la DWORD 0x37373737) allora decifra ulteriori settori sempre con XOR 0x37
9. Al termine chiede di riavviare il computer

Petya.A: il punto debole, come calcolare la key senza pagare

Come abbiamo visto precedentemente, solo i primi 16 caratteri inseriti andranno a formare la Key da 16 byte: B0, B1, B2, B3, B4, B5, B6, B7, B8, B9, B10, B11, B12, B13, B14, B15.

Dalla Key da 16 byte si ottiene una Key da 32 byte, vedi figura precedente, dove:

- $K_i = B_i + 0x7A$
- $K_{i+1} = 2*B_i$

Dalla "Master Table" di 64 byte vengono create 2 tabelle (vettori) uguali di 32 byte: Tab_1 e Tab_2.

Le Tab_1 e Tab_2 sono ottenute prendendo la parte bassa (WORD) delle 16 DWORD della "Master Table". In questo modo si andranno ad utilizzare solo i byte K0, K1, K4, K5, ..., K28, K29 della Key a 32 byte.

La Tab_1 sarà rimescolata dall'algoritmo di Salsa e sommata a 16 bit con la Tab_2 ottenendo una tabella di 16 DWORD contenenti le chiavi XOR per la cifratura (Tab_3).

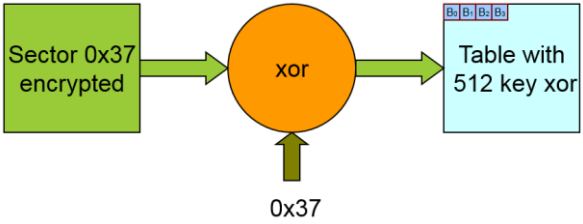
Da questo si evince che Petya utilizza solo 8 dei 16 Byte inseriti nella chiave iniziale, questo ci permette di determinare in modo più agevole la chiave di cifratura utilizzata.

I byte della chiave utilizzati nell'algoritmo di cifratura saranno: B0, B2, B4, B6, B8, B10, B12, B14.

In questo modo siamo passati da una chiave inserita di 16 Byte ad una chiave di 8 Byte, abbassando notevolmente il numero delle possibili combinazioni (54^8).

Vediamo ora come è possbile determinare la chiave senza pagare.

Petya utilizza il settore 0x37 per verificare la correttezza della chiave inserita. Dal settore 0x37 possiamo determinare i valori XOR utilizzati per la cifratura:



Settore 0x37 cifrato:

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
6E00:	FB	C7	37	37	17	2D	37	37	A3	76	37	37	39	42	37	37
6E10:	61	B1	37	37	EC	FF	37	37	53	FF	37	37	FF	45	37	37
6E20:	37	37	37	37	37	77	37	37	55	6D	37	37	0B	26	37	37
6E30:	8F	70	37	37	4D	3A	37	37	D1	94	37	37	DE	FD	37	37
6E40:	FC	C7	37	37	17	2E	37	37	A3	76	37	37	39	C2	37	37
6E50:	E1	B2	37	37	EC	FF	37	37	53	3F	37	37	FF	45	37	37
6E60:	35	09	37	37	37	37	37	37	55	6D	37	37	0B	25	37	37
6E70:	8F	B0	37	37	4D	3A	37	37	D1	93	37	37	DE	FD	37	37
6E80:	FB	C7	37	37	97	2E	37	37	A3	7C	37	37	39	B2	37	37
6E90:	61	B2	37	37	EC	FF	37	37	53	BF	37	37	FF	45	37	37
6EA0:	33	09	37	37	37	B7	37	37	52	6D	37	37	8B	26	37	37
6EB0:	0F	30	37	37	4D	3A	37	37	D1	94	37	37	DE	FD	37	37
6EC0:	FC	C7	37	37	97	2E	37	37	A3	74	37	37	39	C2	37	37
6ED0:	61	B1	37	37	EC	FF	37	37	53	FF	37	37	FF	45	37	37
6EE0:	31	0B	37	37	37	37	37	37	55	6D	37	37	0B	25	37	37
6EF0:	0F	F0	37	37	4D	3A	37	37	D1	94	37	37	DE	FD	37	37
6F00:	FE	C7	37	37	17	2B	37	37	A3	74	37	37	39	42	37	37
6F10:	E1	B2	37	37	EC	FF	37	37	53	7F	37	37	FF	45	37	37
6F20:	3F	37	37	37	37	B7	37	37	55	6D	37	37	8B	26	37	37
6F30:	8F	B0	37	37	4D	3A	37	37	51	92	37	37	DE	FD	37	37
6F40:	FC	C7	37	37	97	EE	37	37	A3	78	37	37	B9	43	37	37
6F50:	E1	B1	37	37	EC	FF	37	37	53	7F	37	37	FF	5F	37	37
6F60:	3D	0D	37	37	37	37	37	37	53	6D	37	37	0B	25	37	37
6F70:	0F	7E	37	37	4D	30	37	37	D1	93	37	37	DD	FD	37	37
6F80:	FE	C7	37	37	97	2E	37	37	A3	74	37	37	39	02	37	37
6F90:	E1	B1	37	37	EC	FF	37	37	53	FF	37	37	FF	45	37	37
6FA0:	3B	33	37	37	37	B7	37	37	52	6D	37	37	8B	26	37	37
6FB0:	8F	30	37	37	4D	3A	37	37	D1	94	37	37	DE	FD	37	37
6FC0:	FE	C7	37	37	97	EC	37	37	A3	7C	37	37	B9	B3	37	37
6FD0:	61	B2	37	37	EC	FF	37	37	53	BF	37	37	FF	5F	37	37
6FE0:	39	0F	37	37	37	77	37	37	53	6D	37	37	0B	25	37	37
6FF0:	0F	7E	37	37	4D	30	37	37	D1	94	37	37	DD	FD	37	37

XOR 0x37

Tabella con le 512 xor key:

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000:	CC	F0	00	00	20	1A	00	00	94	41	00	00	0E	75	00	00	Output Salsa20 con
010:	56	86	00	00	DB	C8	00	00	64	C8	00	00	C8	72	00	00	Contatore = 0 (T 0)
020:	00	00	00	00	00	40	00	00	62	5A	00	00	3C	11	00	00	
030:	B8	47	00	00	7A	0D	00	00	E6	A3	00	00	E9	CA	00	00	
040:	CB	F0	00	00	20	18	00	00	94	41	00	00	0E	F5	00	00	Output Salsa20 con
050:	D6	85	00	00	DB	C8	00	00	64	08	00	00	C8	72	00	00	Contatore = 1 (T 1)
060:	02	3E	00	00	00	00	00	00	62	5A	00	00	3C	12	00	00	
070:	B8	47	00	00	7A	0D	00	00	E6	A4	00	00	E9	CA	00	00	
080:	CC	F0	00	00	A0	19	00	00	94	4B	00	00	0E	B5	00	00	Output Salsa20 con
090:	56	85	00	00	DB	C8	00	00	64	88	00	00	C8	72	00	00	Contatore = 2 (T2)
0A0:	04	3E	00	00	00	80	00	00	65	5A	00	00	BC	11	00	00	
0B0:	B8	07	00	00	7A	0D	00	00	E6	A3	00	00	E9	CA	00	00	
0C0:	CB	F0	00	00	A0	19	00	00	94	43	00	00	0E	F5	00	00	Output Salsa20 con
0D0:	56	86	00	00	DB	C8	00	00	64	C8	00	00	C8	72	00	00	Contatore = 3 (T 3)
0E0:	06	3C	00	00	00	00	00	00	62	5A	00	00	3C	12	00	00	
0F0:	B8	C7	00	00	7A	0D	00	00	E6	A3	00	00	E9	CA	00	00	
100:	C9	F0	00	00	20	1C	00	00	94	43	00	00	0E	75	00	00	Output Salsa20 con
110:	D6	85	00	00	DB	C8	00	00	64	48	00	00	C8	72	00	00	Contatore = 4 (T 4)
120:	08	00	00	00	00	80	00	00	62	5A	00	00	BC	11	00	00	
130:	B8	87	00	00	7A	0D	00	00	66	A5	00	00	E9	CA	00	00	
140:	CB	F0	00	00	A0	D9	00	00	94	4F	00	00	8E	74	00	00	Output Salsa20 con
150:	D6	86	00	00	DB	C8	00	00	64	48	00	00	C8	68	00	00	Contatore = 5 (T 5)
160:	0A	3A	00	00	00	00	00	00	64	5A	00	00	3C	12	00	00	
170:	38	49	00	00	7A	07	00	00	E6	A4	00	00	EA	CA	00	00	
180:	C9	F0	00	00	A0	19	00	00	94	43	00	00	0E	35	00	00	Output Salsa20 con
190:	D6	86	00	00	DB	C8	00	00	64	C8	00	00	C8	72	00	00	Contatore = 6 (T 6)
1A0:	0C	04	00	00	00	80	00	00	65	5A	00	00	BC	11	00	00	
1B0:	B6	07	00	00	7A	0D	00	00	E6	A3	00	00	E9	CA	00	00	
1C0:	C9	F0	00	00	A0	D8	00	00	94	4B	00	00	8E	B4	00	00	Output Salsa20 con
1D0:	56	85	00	00	DB	C8	00	00	64	88	00	00	C8	68	00	00	Contatore = 7 (T 7)
1E0:	0E	38	00	00	00	40	00	00	64	5A	00	00	3C	12	00	00	
1F0:	38	49	00	00	7A	07	00	00	E6	A3	00	00	EA	CA	00	00	

Questa tabella è ottenuta concatenando le prime 8 tabelle di output di Salsa20 variando il campo del contatore da 0 a 7 in input.

Attraverso algoritmi genetici o meta-euristici, come Cuckoo Search, sarà possibile determinare la chiave di cifratura utilizzata. La funzione obiettivo o di costo sarà quella di minimizzare il numero di bit differenti tra la tabella di output generata dalle soluzioni ipotizzate e quella effettiva con contatore 0.

La lunghezza della chiave da cercare è di 8 caratteri e non di 16 o 32.

La soluzione ottima, cioè la chiave di cifratura utilizzata da Petya, sarà quella che avrà costo uguale 0, cioè numero di bit differenti pari a zero.

Per testare se le soluzioni possono evolvere verso l'ottimo, abbiamo messo a confronto le tabelle di output di Salsa20 che sono ottenute variando il contatore da 0 a 7. Questo ci permette di valutare quant'è la variazione in bit dell'output se variamo di 1, 2 o 3 bit l'input. Come si evince dalla tabella le variazioni in output sono minime.

Numero di bit differenti tra le tabelle (output di Salsa20)

	T0	T1	T2	T3	T4	T5	T6	T7
T0	-	25	23	18	18	40	18	36
T1	25	-	22	13	19	29	27	35
T2	23	22	-	19	25	39	13	29
T3	18	13	19	-	24	30	18	28
T4	18	19	25	24	-	38	16	42
T5	40	29	39	30	38	-	36	16
T6	18	27	13	18	16	36	-	34
T7	36	35	29	28	42	16	34	-

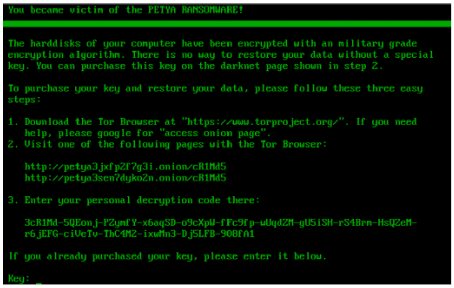
Questo ci permette di determinare la chiave di cifratura di Petya in pochi secondi.

Petya.B: green version

A maggio 2016 viene rilasciata la versione "B" di Petya chiamata "green" version per il suo colore di layout. Nella precedente versione il dropper di Petya necessitava di essere eseguito con i diritti di administrator per infettare l'MBR. Se l'utente non disponeva di tali privilegi o l'User Account Control era attivo, il dropper di Petya non era in grado di infettare l'MBR e di conseguenza di cifrare la Master File Table.

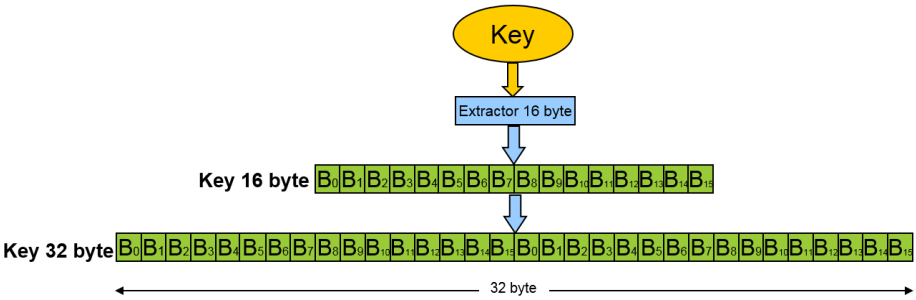
Per ovviare a questa problematica di non perdere questa chance di cifrare il contenuto del computer, nella nuova release "B" di Petya, se il dropper veniva eseguito senza i diritti di Administrator, il malware non andava ad infettare l'MBR, ma eseguiva un altro ransomware, chiamato Mischa, che andava a cifrare i file di documenti e dati nelle modalità consuete.

Nel caso che il dropper fosse stato eseguito con i diritti di Administrator, andava ad infettare l'MBR con Petya e cifrava l'MFT, ma in questo caso il ransomware Mischa non veniva eseguito.



In questa nuova versione di Petya viene utilizzato l'algoritmo di cifratura Salsa20 con operazioni a 32 bit, ma vengono commessi ancora errori durante l'applicazione dell'algoritmo di cifratura.

La password della Key iniziale è ancora di 16 byte, che diventano 32 caratteri concatenando i primi 16 con se stessi: *<psw 16><psw 16>*.



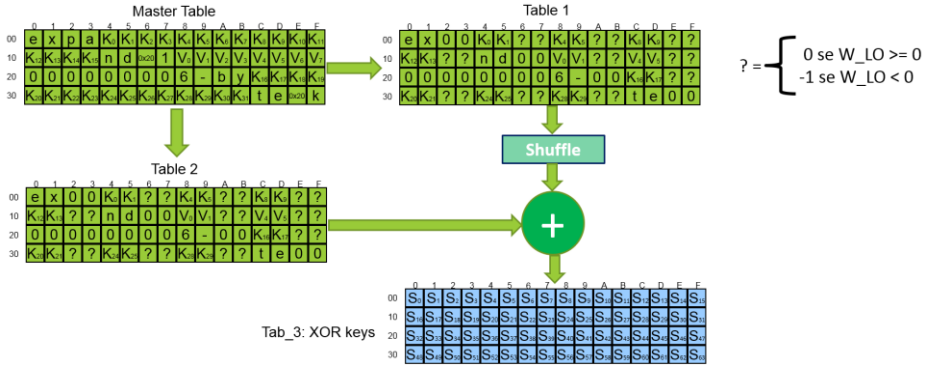
L'algoritmo di cifratura utilizzato è Salsa20, questa volta l'autore ha applicato correttamente le operazioni a 32 bit, ma ha commesso un errore. Nella creazione delle tabelle di input di Salsa20 ha commesso un errore nell'utilizzo assembly dell'istruzione CWD:

```
0:5C22  push   bp
0:5C23  mov    bp, sp
0:5C25  push   si
0:5C26  mov    si, [bp+arg_0]
0:5C29  sub    al, al
0:5C2B  mov    ah, [si+1]
0:5C2E  mov    cl, [si]
0:5C30  sub    ch, ch
0:5C32  add    ax, cx
0:5C34  cwd
0:5C35  pop    si
0:5C36  leave
0:5C37  retn
```

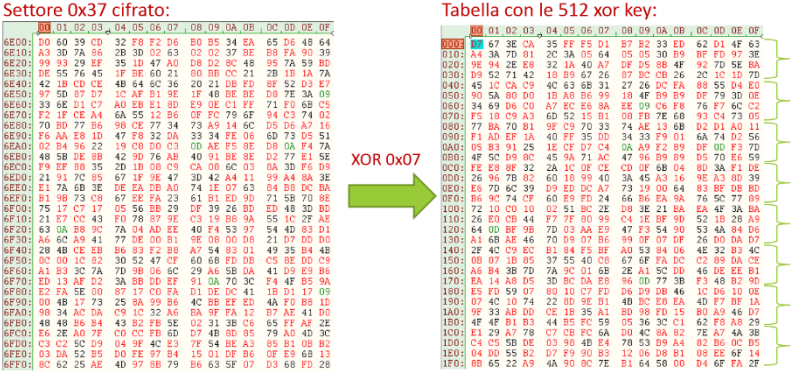
che comportava la sovrascrittura della word più significativa con il segno della word meno significativa, questo implicherà che solo 8 caratteri su 16 della password saranno coinvolti nella fase di cifratura.
Anche nella versione precedente aveva commesso un simile errore.
Errare è umano, perseverare è diabolico!

Vediamo ora lo schema di cifratura con Salsa20 con operazioni a 32 bit e l'errore nell'utilizzo dell'istruzione assembly CWD. Le 2 tabelle 1 e 2, che dovrebbero essere una copia "fedele" della Master Table, con l'errore commesso, risultano essere modificate nella word più significativa dal

segno della word meno significativa, andando a sovrascrivere una parte della chiave utilizzate nella cifratura.



L'errore commesso non va ad influire sulla robustezza di Salsa20, che restituisce una tabella di output senza valori nulli. Ma è possibile sfruttare l'errore commesso per determinare la chiave di cifratura senza pagare il riscatto.



Come nella versione precedente il settore 0x37 è utilizzato per verificare la correttezza della chiave inserita, questa volta l'operazione è un XOR 0x07, da cui si ottengono le 8 tabelle di output di Salsa20 variando il campo del contatore da 0 a 7 in input. La robustezza di Salsa20 però non ci permette di applicare algoritmi genetici o metaeuristici per determinare la chiave

inserita, come possiamo vedere dalla variazioni in bit delle tabelle di output (variando il campo del contatore da 0 a 7 in input):

Numero di bit differenti tra le tabelle (output di Salsa20)

	T0	T1	T2	T3	T4	T5	T6	T7
T0	-	259	256	247	279	258	262	271
T1	259	-	253	274	254	263	257	268
T2	256	253	-	269	269	258	258	253
T3	247	274	269	-	260	245	255	242
T4	279	254	269	260	-	243	277	246
T5	258	263	258	245	243	-	242	253
T6	262	257	258	255	277	242	-	255
T7	271	268	253	242	246	253	255	-

Minime variazioni di qualche bit in input generano variazioni del 50% dei bit in output, dai test effettuati le soluzioni evolvevano fino ad un massimo di 180 bit differenti.

L'unica soluzione che ci rimane è quella di eseguire un brute force delle soluzioni, sfruttando l'errore che il numero di caratteri della chiave coinvolti nella cifratura sono 8 e la dimensione dell'alfabeto è di 54 caratteri. Questo ci porta ad avere un valore massimo di combinazioni pari a 54^8, che ci permette di ottenere la soluzione anche nel caso peggiore in qualche settimana.

Petya.C: Ransomware as Service

A luglio 2016 viene rilasciata la versione "C" di Petya, dove viene corretto l'ultimo errore riscontrato nella precedente release, da cui si poteva risalire alla chiave di cifratura attraverso un attacco brute force. Anche questa variante utilizza la medesima interfaccia della "green" version.

Da questa release non è più possibile determinare la chiave di cifratura senza pagare il riscatto. La novità di questa nuova versione è la fornitura di Petya & Mischa come servizio. Per diventare affiliati al servizio è necessario registrarsi al costo simbolico di 1 $. L'affiliato dovrà distribuire Petya &

Mischa attraverso le proprie campagne, il profitto ottenuto sarà in base ai pagamenti dei riscatti incassati.

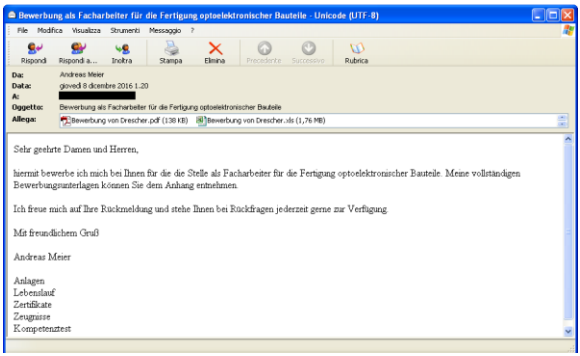
In base al volume settimanale di pagamenti di riscatti ottenuti dall'affiliato per la distribuzione/infezioni di Petya & Mischa, le quote di profitto saranno ripartite come indicato da questa tabella:

Petya.D: Doppio riscatto con Mischa e Petya

A dicembre 2016 l'autore di Petya si fa vivo con la nuova versione Goldeneye 4.0. A partire dal 6 dicembre, vi è stata in Germania una campagna di spam che diffondeva la versione Goldeneye di Petya via posta elettronica.

La campagna spam veniva confermata in un tweet da Janus, autore di Petya Goldeneye il 7 dicembre.

Come nelle campagne precedenti di Petya, il messaggio di posta elettronica fa riferimento sempre alla ricerca di personale. In questo caso l'email è una candidatura per un posto di lavoro nella produzione di dispositivi optoelettronici.



Il messaggio infetto da Petya contiene 2 allegati:

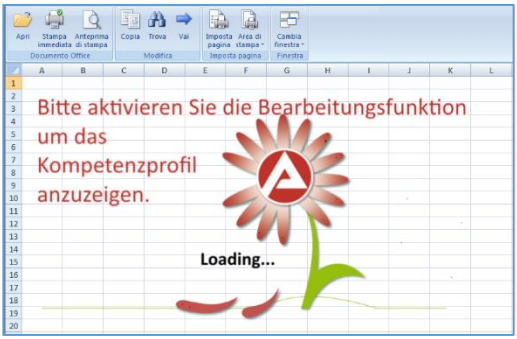
- “Bewerbung von Drescher.xls” (dimensione: 1804800 byte, MD5: FEF25AFCCEBE63858C093CB716D03203)
- “Bewerbung von Drescher.pdf” (dimensione: 138540 byte, MD5: 16E41EBD9414E9327E9D447E4B5A6FE4)

Il file “Bewerbung von Drescher.xls” contiene delle macro di Excel, che creano ed eseguono dalla cartella %temp% il seguente file:

- Nome: rad0A3AB.exe
- Dimensione: 368640 byte
- MD5: 08828DAF9A027E97FEE2421AC6CBC868

L'apertura del documento “Bewerbung von Drescher.xls”, con le macro attive, comporta l'esecuzione del file rad0A3AB.exe dalla cartella di %temp%.

In questa prima fase viene eseguito il ransomware *Mischa* che cifrerà ogni file documento all'interno della cartella c:\user(%user%) di Windows.



I file di documento cifrati saranno rinominati aggiungendo una nuova estensione casuale di 8 caratteri: Cartel1.xlsx ==> Cartel1.xlsx.*rCazhYJU*

Il ransomware Mischa rilascerà in ogni sottocartella di %user% il file "*YOUR_FILES_ARE_ENCRYPTED.TXT*" con le istruzione del riscatto:

You became victim of the GOLDENEYE RANSOMWARE!

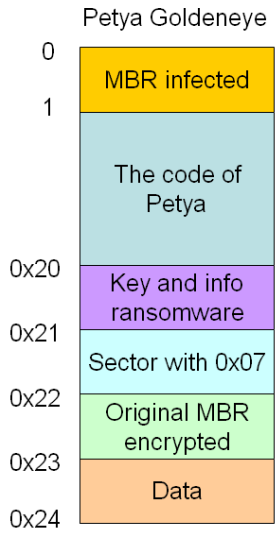
The files on your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".

2. Visit one of the following pages with the Tor Browser:
http://golden5a4eqranh7.onion/rCazhYJU http://goldeny4vs3nyoht.onion/rCazhYJU

3. Enter your personal decryption code there: rCazhYJUF1pRVywmEsuUe[..]

Dopo che il ransomware Mischa ha terminato la cifratura dei file di documento all'interno della cartella %user%, Goldeneye esegue il ransomware Petya.



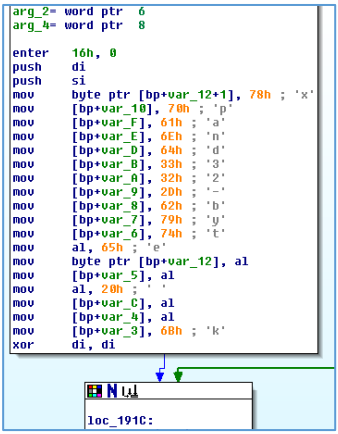
Il dropper di Petya (rad0A3AB.exe) è in grado di bypassare il livello intermedio dell'User Account Control (UAC), andando ad infettare il Master Boot Record del disco fisso sovrascrivendo i primi 36 settori, come rappresentato nello schema.
Il settore 0 dell'MBR è infettato dal codice di loader di Petya. Dal settore 1 al 0x20 troviamo il codice virale di Petya. Il settore 0x20 contiene la chiave di cifratura di 32 byte, il vettore di inizializzazione e gli indirizzi Tor-Onion e l'ID della vittima. Il settore 0x21, nella prima fase, è riempito solo con il byte 0x07.
Il settore 0x22 contiene il Master Boot Record cifrato con xor 0x07 e il settore 0x23, in questa fase contiene solo 0.

Al termine di questa fase Petya Goldeneye simula una schermata blu di errore (BSOD).

Durante la fase 1, Petya Goldeneye non ha ancora iniziato a cifrare la Master File Table (MFT), ma ha solamente infettato il Master Boot Record. Se è stato disattivato il riavvio automatico del computer in caso di BSOD, il computer infettato da Petya rimarrà bloccato con la schermata di errore BSOD. Se siamo in questa situazione con la schermata BSOD è possibile spegnere il computer e riavviarlo da un CD\DVD "bootabile" di Windows per eseguire un "fixmbr" per rimuovere Petya dal Master Boot Record. Se invece il computer viene riavviato o si è riavviato in automatico, allora verrà eseguito il boot loader dell'MBR infetto da Petya che darà inizio alla fase 2 della cifratura della Master File Table.

La fase 2 di Petya ha inizio con il primo boot, il codice dell'MBR viene caricato all'indirizzo 0:7c00. L'MBR infetto da Petya va a leggere 0x20 settori partendo dal settore 1 e li carica all'indirizzo 0:8000.

Se il primo byte del settore 0x20, cioè quello del campo "stato del disco", vale 0, allora inizierà la procedura di cifratura della Master File Table di ogni partizione del disco.

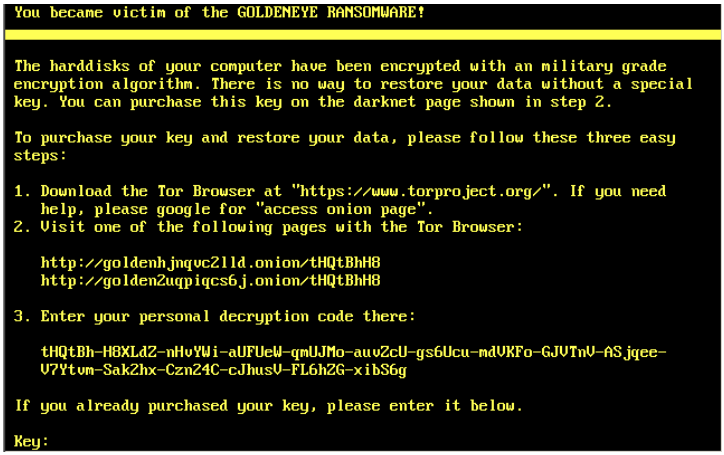


L'algoritmo di cifratura utilizzato è ancora Salsa20, qui possiamo vedere la routine di inizializzazione dell'array di input di Salsa20 con il valore: expand 32 byte k.

In questa fase Petya visualizza un falso chkdsk che, in realtà, sta cifrando la Master File Table. La percentuale visualizzata indica la porzione di Master File Table cifrata.

Al termine del chkdsk il computer si riavvia in automatico, visualizzando la nuova versione di Petya GoldeEye:

Premendo un tasto, ci viene indicato che siamo vittima di GOLDENEYE RANSOMWARE:



Petya Goldeneye ci indica quali sono i siti per pagare il riscatto e l'ID della vittima. A questa punto Petya rimane in attesa dell'inserimento della chiave per decifrare l'MFT.

La chiave da inserire manualmente è una stringa di 32 caratteri presi dal seguente insieme: 0123456789abcdef

Da questa chiave di 32 caratteri, Petya eseguirà ulteriori operazioni per ottenere una nuova chiave definitiva di 32 byte.

Petya per verificare la correttezza di quest'ultima chiave di 32 byte, ottenuta da quella inserita, proverà a decifrare il settore 0x21, se ogni byte del settore dopo la de-cifratura avrà il valore 0x07 allora la chiave che è stata inserita è corretta e procederà alla decifratura dell'MFT.

Collegandosi con il browser Tor-Onion ai siti indicati è possibile sapere dell'ammontare del riscatto da pagare.

Questa nuova versione di Petya Goldeneye ha raddoppiato la richiesta di riscatto per ri-ottenere l'usabilità del proprio PC prima e dei propri file poi:

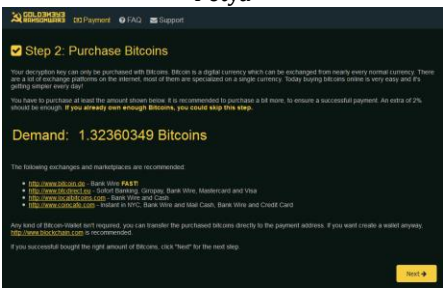
- Petya cifrando la MFT chiede un primo riscatto per decifrarla;
- Mischa cifrando i file di dati chiede un ulteriore riscatto per decifrarli.

Nelle versioni precedenti di Petya la cifratura dell'MFT era eseguita solo nel caso in cui il dropper veniva lanciato con i diritti di Administator, ed in caso contrario comportava la cifratura solo dei file di documenti attraverso il ransomware Mischa.

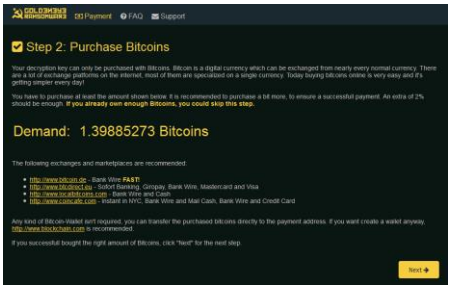
Questa nuova release esegue in serie prima il ransomware Mischa, e dopo è in grado by-passare il livello intermedio dell'User Account Control (UAC) andando ad infettare il Master Boot Record.

La malcapitata vittima si troverà di fronte al pagamento sia del riscatto per decifrare la Master File Table sia del riscatto per decifrare i file criptati da Mischa. Nel nostro test i riscatti richiesti sono stati rispettivamente di 1,39 e 1,32 Bitcoin come indicato nelle 2 figure:

Petya



Mischa



Come già evidenziato l'autore di Petya si fa chiamare Janus.

Janus è un fan di James Bond e in particolar modo del film "Goldeneye", infatti tutti i nomi indicati come Petya, Mischa, Janus sono citati in Goldeneye. Inoltre l'autore di Petya ha 2 account su twitter:

- @JanusSecretary
- @janussec

A Janus piace "giocare", burlandosi della Polizia tedesca di Osnabruck, scambiandosi tweet sul ransomware Goldeneye:

CrySis: Saraswati

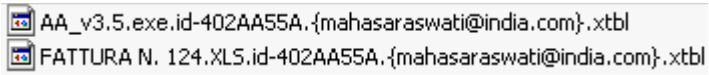
Anno	2016 maggio
Estensione	ID-<numero>.<email>.xtbl
Algoritmo	RSA - AES
Riscatto	Dipende dalla versione
Rete	email

All'inizio del 2016 vengono identificate le prime versioni del ransomware CrySis. Questo tipo di malware usa diverse estensioni aggiungendoci un ID seguito dall'indirizzo email a cui richiedere il riscatto, per terminare con l'estensione .XTBL. Sono state riscontrate diverse tipologie che utilizzano svariati temi di ransomware.

A maggio 2016 gli autori di CrySis si sono ispirati all'India ed in particolar modo alla divinità indiana Saraswati.

CrySis utilizza diversi vettori d'infezione come gli exploit kit, ma il suo cavallo di battaglia è l'attacco ai desktop remoti dei server. Il principale metodo utilizzato è quello di accedere attraverso il desktop remoto al server attraverso le credenziali dell'utente e di eseguire manualmente il ransomware sul server della vittima.

Il ransomware Saraswati cifra ogni file di documento (come .txt, .doc, .ppt, .mdb, .xls, etc), ma anche file .EXE, e li rinomina aggiungendo l'estensione: .id-????????.{mahasaraswati@india.com}.xtbl:



dove ???????? corrisponde un numero esadecimale dell'ID della vittima. Per decifrare i file è necessario inviare una richiesta via email a: mahasaraswati@india.com.

Questa variante di CrySis “Saraswati” si presenta con il nome *saraswati.exe* e viene copiato all'interno di cartella roaming dell'utente %user%\appdata\roaming\:

- NOME FILE: saraswati.exe
- DIMENSIONE: 114688 byte
- MD5: 67f54ddc01178bb5878fe14a567813fc

Nome del progetto trovato all'interno del crypto-malware: C:\crysis\Release\PDB\payload.pdb

Saraswati si mette in esecuzione automatica aggiungendo la seguente chiave di registro:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

[lttmrsuc] = %windir%\System32\Saraswati.exe

Modifica il menu di avvio per mettersi in esecuzione automatica e visualizzare le istruzioni del riscatto in formato txt e jpg:

%user%\Menu Avvio\Programmi\Esecuzione automatica\Saraswati.exe

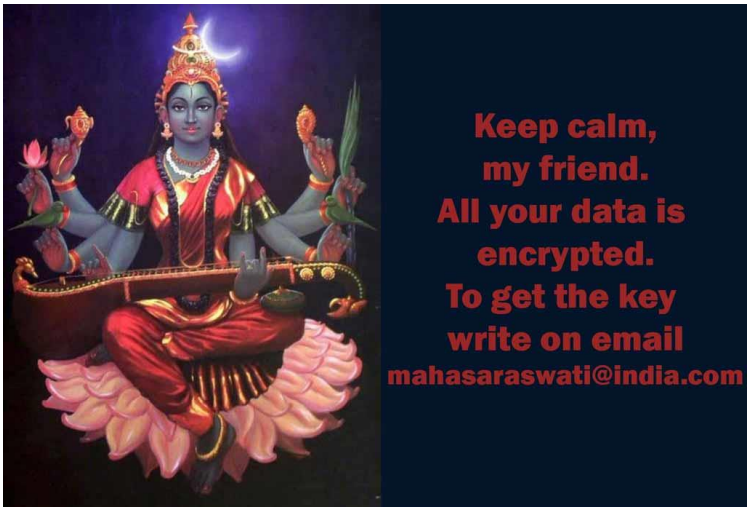
%user%\Menu Avvio\Programmi\Esecuzione automatica\How to decrypt your files.jpg

%user%\Menu Avvio\Programmi\Esecuzione automatica\How to decrypt your files.txt

Sul desktop dell'utente viene copiato il file: “How to decrypt your files.txt”

To decrypt your data write me to mahasaraswati@india.com

Nella cartella dell'utente viene copiato il file: “How to decrypt your files.jpg”



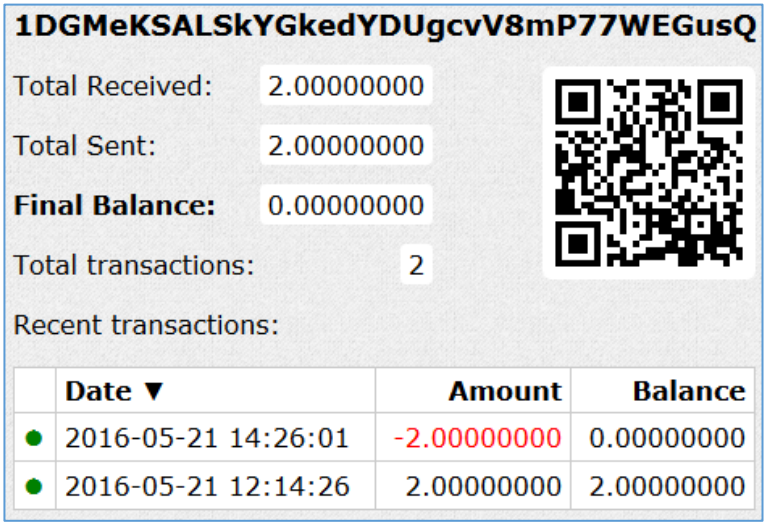
Abbiamo inviato una mail all'indirizzo indicato e questa è stata la loro risposta:

We are writing to inform you that our team of network security specialists has analyzed your system and has identified vulnerabilities in the protection.
We kindly draw your attention that defensive operation on your computer is not running properly and now the whole database is at risk.
All your files are encrypted and can not be accepted back without our professional help.
Obviously vulnerability analysis, troubleshooting, decoding the information and then ensuring safety are not a simple matter.
And so our high-grade and quick service is not free.
Please note that today the price of your files recovery is 3 Bitcoins, but next day it will cost 5 Bitcoins.
You should buy bitcoins here https://localbitcoins.com/faq
Read the paragraphs:
1. How to buy Bitcoins?
2. How do I send Bitcoins and how can I pay with Bitcoins after buying them?
The Bitcoin wallet for payment is 1DGMeKSALSkYGkedYDUgcvV8mP77WEGusQ
After the transfer of bitcoins please send email with screenshot of the payment page.
We does not advise you to lose time, because the price will encrese with each passing day.
As proof of our desire and readiness to help you, we can decipher a few of your files for test.
To check this you can upload any encrypted file on web site dropmefiles.com, size no more than 10 MB (only text file or a photo) and send us a download link.
Certainly after payment we guarantee prompt solution of the problem, decrypt the database to return to its former condition and consultation how to secure the rules of the system safety.

Kind regards, Saraswati.

Secondo i criminali i file criptati da Saraswati per essere decifrati necessitano del pagamento di un riscatto pari a 3 BitCoin, ma il riscatto salirà a 5 BitCoin dal giorno successivo.

E' interessante verificare quante persone hanno pagato il riscatto verso il portafoglio indicato: *1DGMeKSALSkYGkedYDUgcvV8mP77WEGusQ*



1DGMeKSALSkYGkedYDUgcvV8mP77WEGusQ

Total Received:	2.00000000
Total Sent:	2.00000000
Final Balance:	0.00000000
Total transactions:	2

Recent transactions:

	Date ▼	Amount	Balance
●	2016-05-21 14:26:01	-2.00000000	0.00000000
●	2016-05-21 12:14:26	2.00000000	2.00000000

Dal report del portafoglio indicato dove pagare il riscatto, solo una transazione di 2 BTC è stata versata.

Nel 2016 diverse sono le varianti di CrySis che sono state diffuse via exploit kit o attacchi via RDP (Desktop Remoto):

- Vegclass@aol.com or Greebin@india.com
- mkgoro@india.com (Dharma)
- Veracrypt@india.com

Nel prosieguo torneremo ancora sui portafogli di CrySis.

Anubis

Anno	2016 ottobre
Estensione	.coded
Algoritmo	RSA - AES
Riscatto	2,5 BTC che dopo un giorno passa 3 BTC
Rete	email

Dopo la divinità indiana Saraswati, gli autori di ransomware si sono ispirati all'antico Egitto. A ottobre 2016 dall'Egitto, ma via Panama, arriva Anubis!

Il malware si presenta con il nome di ANUBIS.EXE, ma non sono noti i vettori d'infezione utilizzati per diffondersi.

- Nome file: ANUBIS.EXE
- Dimensione file: 117248 byte
- MD5:104d38009f6b36bab64b625735907c88

Anubis durante l'esecuzione genera un ID per il computer che verrà inviato al server di C&C 190.14.37.177 (localizzato a Panama) insieme al nome dell'utente e il nome del PC attraverso una richiesta POST alla seguente pagina: http://190(dot)14(dot)37(dot)177/rs/createkeys.php

```
Form item: "idnumber" = "jPhHt30nkKhGBBYKzo1d"
Form item: "username" = "XXXXXX"
Form item: "pcname" = "XXXXXX-PC"
```

in risposta viene mandato una chiave RSA che verrà utilizzato per cifrare la chiave AES.

Ora Anubis esegue una richiesta POST alla seguente pagina: http://190(dot)14(dot)37(dot)177/rs/savekey.php

```
Form item: "idnumber" = "jPhHt30nkKhGBBYKzo1d"
Form item: "pcname" = "XXXXXX-PC"
Form item: "aesencrypted" =
"UslM29xzZfq4HRnwmwJ/vSi/vFSSZmdFJ7sAyEELB90eJaMVtb80hs2XnrPTou7SdixLEH8
+XJRSsF0i5SgwThx5Fpv6i7epOTjgLcw70a+e5q7+OA2XRvipKiQVbHUdBiBtqSlcBl20Mov7
R9FTOSMrmPC9UGFSG4MUbqeJhpeqpjGpVU0i/oEXU1FjVXMwXUr4v6e9sOmgGIM2wQ"
```

Dove vengono inviate le informazioni relative a *idnumber*, *pcname* e *aesencrypted*.

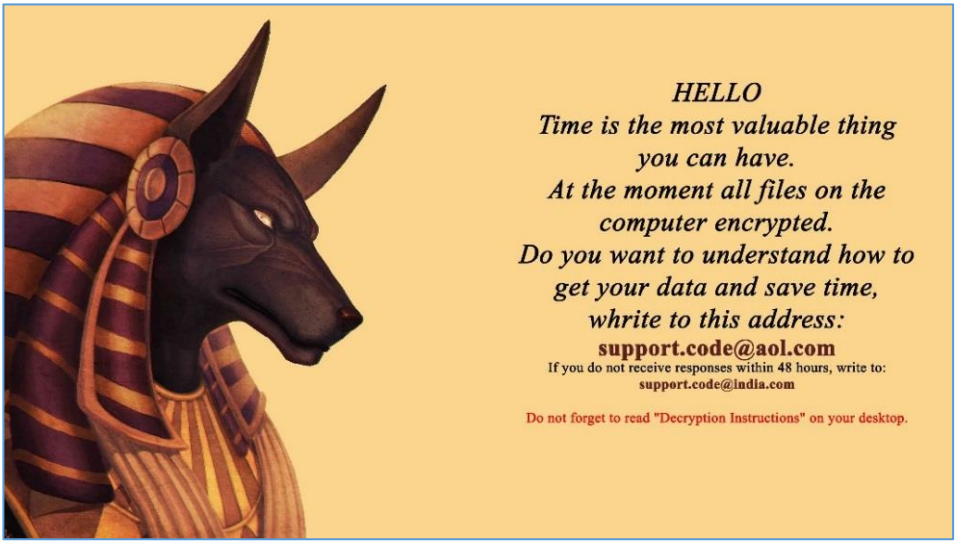
Anubis cifra i file con estensioni, come quelle riportate nella tabella sottostante, e li rinomina aggiungendo al nome originale l'estensione .coded.

```
.3dm, .3ds, .3g2, .3gp, .602, .aes, .arc, .asc, .asf, .asm, .asp, .avi, .bak, .bat, .bmp, .brd, .cgm, .cmd, .cpp, .crt, .csr,
.csv, .dbf, .dch, .dif, .dip, .djv .djvu, .doc .docb .docm .docx, .dot .dotm, .dwg .dotx, .exe, .fla, .flv, .frm, .gif, .gpg,
.hwp, .ibd, .iso, .jar .java .jpeg, .jpg, .key, .lay .lay6, .ldf, .lnk, .log, .m3u, .m4u, .max, .mdb, .mdf, .mid, .mkv,
.mov, .mp3, .mp4, .mpeg, .mpg .ms11, .myd, .myi, .nef, .odb, .odg, .odp, .ods, .odt, .otg, .otp, .ots, .ott, .p12,
.paq, .pas, .pdf, .pem, .php, .png, .pot .potm .potx .ppam, .pps .ppsm .ppsx, .ppt .pptm .pptx, .psd, .rar, .raw,
.rtf, .sch .sldm .sldx, .slk, .stc, .std, .sti, .stw, .svg, .swf, .sxc, .sxd, .sxi, .sxm, .sxw, .sql .sqlitedb, .tar, .tbk, .tgz,
.tif .tiff, .txt, .uop, .uot, .vbs, .vdi, .vmdk, .vmx, .vob, .wav, .wb2, .wk1, .wks, .wma, .wmv, .xlc, .xlm, .xls .xlsb
.xlsm .xlsx, .xlt .xltm .xltx, .xlw, .zip, .7z
```

Il cripto-Malware genera sul desktop della vittima un file *"Decryption Instructions*" (privo di estensione) contenente le istruzioni per pagare il riscatto e rimane in esecuzione:

```
IMPORTANT INFORMATION!
---------------------------
Your Computer ID: jPhHt30nkKhGBBYKzo1d <---- Remember it and send to my email.
---------------------------
All your files are encrypted strongly.!
- How to open my file?
- You need Original KEY and Decrypt Program
- Where can i get?
- Email to me: support.code@aol.com or support.code@india.com
(Open file Decryption Instructions on your Desktop and send your SID)
```

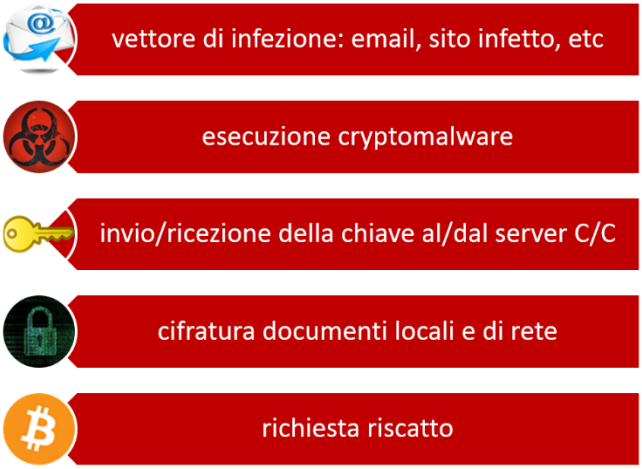
Viene scaricato sempre dallo stesso indirizzo immagine "ransom.jpg" nella cartella dell'utente:



Inviando un'email a *support.code@aol.com* si viene a conoscenza che il costo per aver il programma e la chiave per recuperare i file è di 2.5 BTC poco meno di 1500 €, ma dopo un giorno passano a 3 BTC.

Come Funzionano i Crypto-Malware

Analizziamo ora quali siano i passi eseguiti dai ransomware (Crypto-Malware) durante la fase di attacco.



I crypto-malware vengono veicolati attraverso le varie tipologie di vettori di infezione descritte precedentemente come, ad esempio attraverso campagne di spam via email o sfruttando gli exploit kit durante la navigazione su siti compromessi. Quando il dropper del ransomware raggiunge il computer della vittima, il passo successivo è l'esecuzione del payload. La vittima infettata dal dropper andrà ad installare ed eseguire il payload del Crypto-Malware.

Abbiamo visto nella prima versione di Petya, che il dropper aveva successo se, e solo se, veniva eseguito con i diritti di Administrator. Per gli autori dei ransomware, dopo che è stato raggiunto il computer della vittima, non riuscire ad eseguire o far eseguire il crypto-malware, significherebbe aver compromesso l'attacco e aver perso la chance di cifrare i file e di poter richiedere il riscatto. La maggior parte dei ransomware non necessitano dei diritti di Administrator, poiché anche i soli privilegi dell'utente "guest" sono sufficienti per sferrare l'attacco di cifratura ai file di documenti.

In base alla tipologia del ransomware questo può generare casualmente una chiave che verrà inviata al server di Comando e Controllo oppure può ricevere dal server di Comando e Controllo la chiave per cifrare i file. Alcuni ransomware come il TeslaCrypt o l'Odin (Locky) possono lavorare offline, senza connessione di rete. Questi crypto-malware dopo aver generato la propria chiave privata di cifratura, lasciano nel computer della vittima un ID che include la chiave pubblica.

Ottenuta la chiave di cifratura, il Crypto-Malware inizia a criptare tutti i file di documenti locali e/o di rete in base alla tipologia. Quando ha completato le sue operazioni di cifratura, alcune famiglie di ransomware si possono cancellare, ma lasciano comunque le istruzioni per il riscatto.

Di solito le istruzioni del riscatto vengono lasciate sul desktop in un file di testo o pagina html/hta. Alcune volte viene modificato anche lo sfondo del desktop con un'immagine bitmap riportante la richiesta del riscatto. Nella richiesta di riscatto vengono riportati l'ID della vittima, l'indirizzo del portafoglio in bitcoin (conto corrente) dove pagare la somma richiesta e gli indirizzi Tor-Onion con le modalità di pagamento.

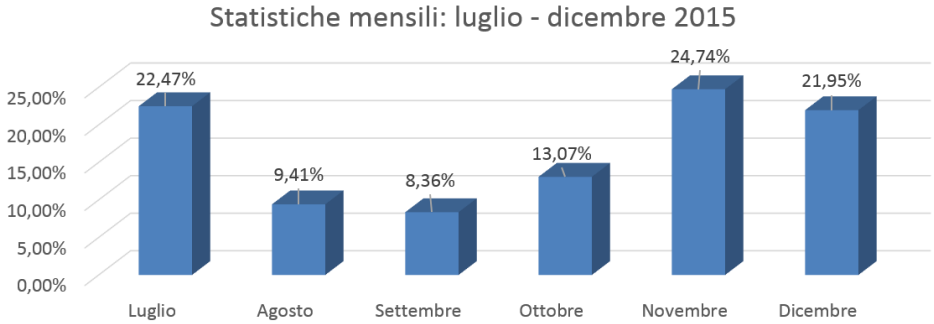
Il ransomware è una minaccia atipica che differisce dai tradizionali malware. E' gestito da organizzazioni criminali, con l'unico obiettivo di guadagnare denaro attraverso la richiesta di una "piccola" somma in bitcoin. Dispongono di un'infrastruttura che permette di rilasciare velocemente nuove varianti, in modo da by-passare il controllo degli antivirus. Al ransomware è sufficiente essere eseguito solo una volta per perpetrare il proprio scopo: la cifratura dei documenti. Se l'antivirus lo dovesse riconoscere anche solamente dopo 2 ore dal completamento della cifratura, ormai il danno è stato compiuto con la criptazione dei file e la protezione antivirus sarebbe inefficace.

Statistiche degli attacchi ransomware in Italia

Il C.R.A.M. ha raccolto ed elaborato dati esclusivamente riferiti ai casi di assistenza compiuti collegandoci al computer della vittima, dove è stato verificato con esattezza la tipologia di ransomware e il numero di file cifrati. Altri studi riportano come statistiche i vettori di infezioni (e-mail, expolit kit, etc.) che rappresentano i tentativi di attacco e non gli attacchi finalizzati cioè quelli dove il ransomware è stato effettivamente eseguito ed e riuscito a cifrare i file in tutto o in parte.

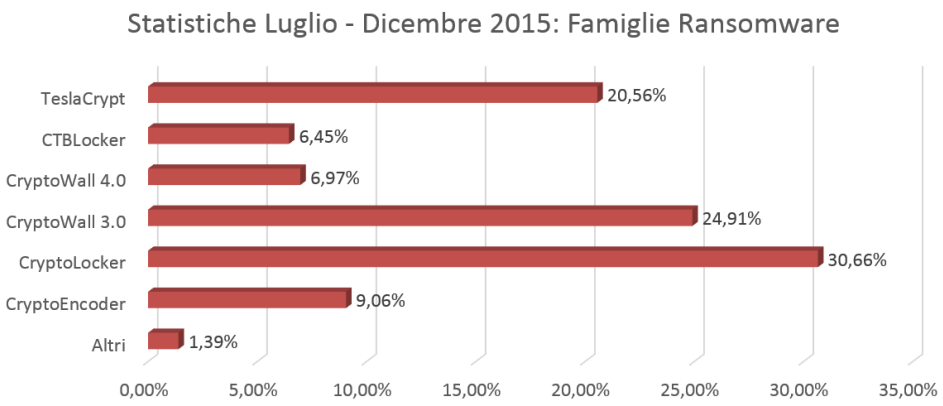
Statistiche da luglio a dicembre 2015

Elaboriamo ora le statistiche dei crypto-malware in Italia negli ultimi 6 mesi del 2015. I casi indagati sono tutti e soli quelli che abbiamo verificato collegandoci in assistenza remota al computer della vittima.



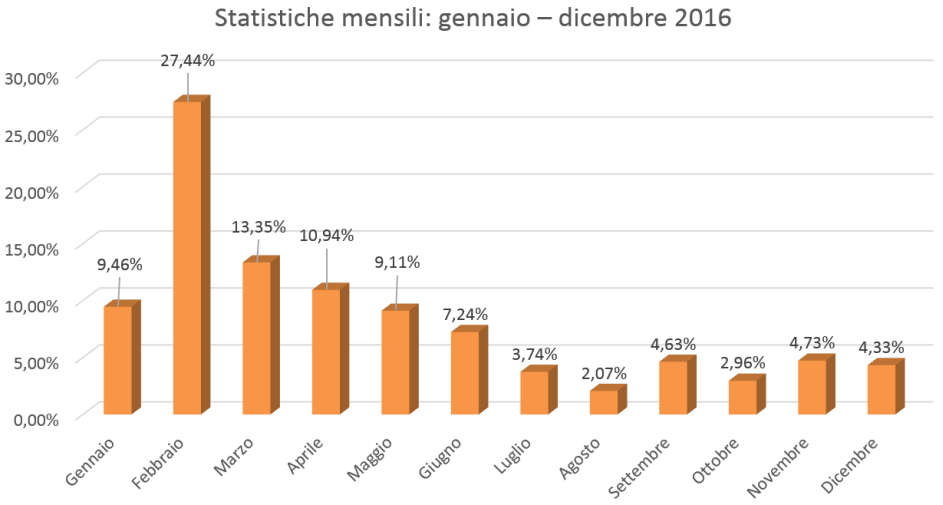
Il crypto-malware più diffuso è stato il CryptoLocker, seguito da CryptoWall 3.0 e dal TeslaCrypt.

E' interessante evidenziare che se andassimo a sommare gli attacchi di CryptoWall 3.0 e 4.0, quest'ultimo rilasciato a settembre 2015, la famiglia CryptoWall (24,91+6,97=31,88%) sarebbe stata quella con maggiore diffusione nel secondo semestre 2015 spodestando CryptoLocker (30,66%). Nel 2015, inoltre, si diffonde in modo non trascurabile TeslaCrypt (20,56%) che re-incontreremo prepotentemente nel 1° quadrimestre 2016.



Statistiche 2016

Nel 2016 i casi di attacchi da ransomware analizzati dal C.R.A.M., rispetto al 2015, sono più che raddoppiati.

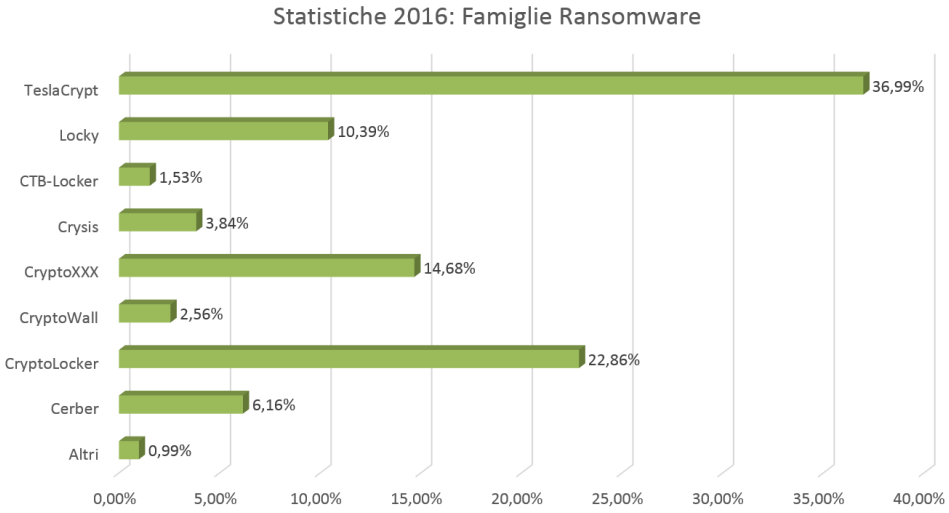


Nei primi 3 mesi dell'anno sono stati rilevati il maggior numero di infezioni. Nel solo mese di febbraio si è riscontrato il picco di infezioni numericamente di poco inferiore agli attacchi indagati complessivamente nel 2° semestre 2015, la maggior parte è stata sferrata da TeslaCrypt.

Nei mesi successivi il numero di segnalazioni è calato progressivamente, fino a toccare il punto più basso ad agosto. Il 3° quadrimestre 2016 ha avuto un andamento pressoché costante, tranne il mese di ottobre dove vi è stata una flessione.

Il 2016 ha visto l'intrecciarsi di "vecchie" conoscenze con le new-entry e alcuni, clamorosi, colpi di scena, da CryptoLocker a TeslaCrypt, da CryptoXXX a Locky.

Sì è anche riscontrato un notevole aumento di nuove famiglie di ransomware rispetto al 2015. Molte di queste famiglie hanno preso il posto di noti ransomware, ma vi è stato anche un non trascurabile sviluppo di crypto-malware, forse sperimentali, di bassa qualità, molto probabilmente realizzati da neofiti, ispirati a movie come Jigsaw, serie televisive come Mr. Robot (FSociety) o giochi come PokemonGo.

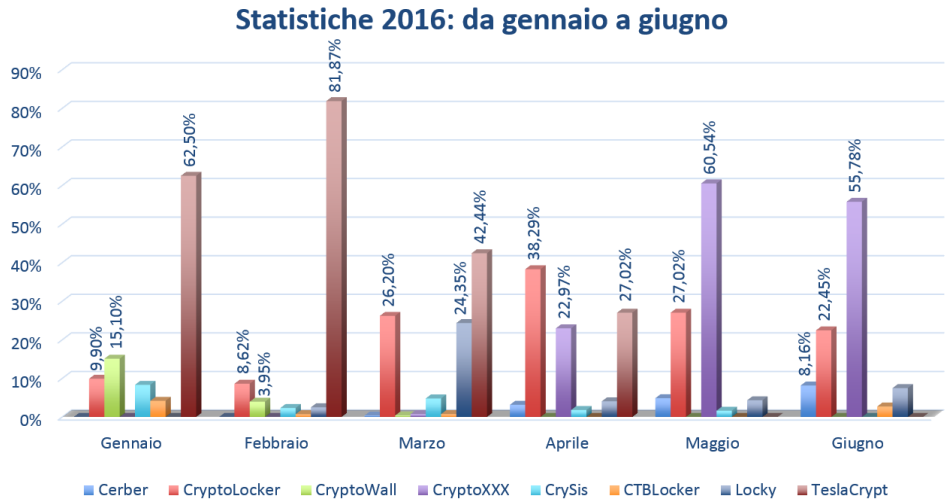


Nel 2016 il ransomware più diffuso in Italia è stato il TeslaCrypt (36,99%), seguito da CryptoLocker alias TorrentLocker (22,86%), sul terzo gradino troviamo CryptoXXX (14,68%). Medaglia di legno per Locky (10,39%),

spauracchio degli ospedali americani, e non solo, con le sue numerose varianti: Zepto, Odin, Osiris e altre.

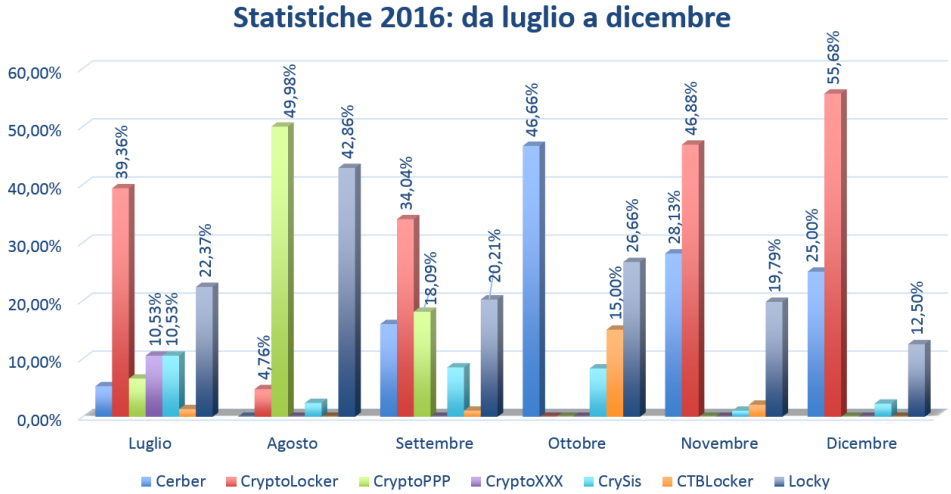
Il TeslaCrypt è il ransomware dell'anno 2016, non solo perché era indecifrabile, ma per il numero di infezioni realizzate in soli 4 mesi da gennaio ad aprile. A maggio 2016 il progetto TeslaCrypt viene chiuso inspiegabilmente, rilasciando pubblicamente la master key per decifrare i file compromessi da tutte le varianti di questo ransomware.

Vediamo ora più in dettaglio l'evoluzione delle principali famiglie di ransomware del 2016 mese dopo mese. Nella figura sotto l'evoluzione relativa al 1° semestre 2016.



Nella seconda metà di gennaio viene rilevata, anche in Italia, la prima ondata del TeslaCrypt 3.0 (62,50%), seguita poi da quella del 1° febbraio che si è prolungata fino a fino mese. TeslaCrypt è indiscutibilmente il ransomware del mese di febbraio con oltre l'80% di infezioni. A marzo TeslaCrypt (42,44%) ha continuato con i suoi attacchi, seguito da CryptoLocker (26,20%) e da Locky (24,35%). Ad aprile vi è la flessione del TeslaCrypt (27,02%), dove il CryptoLocker (38,29%) si riprende la prima

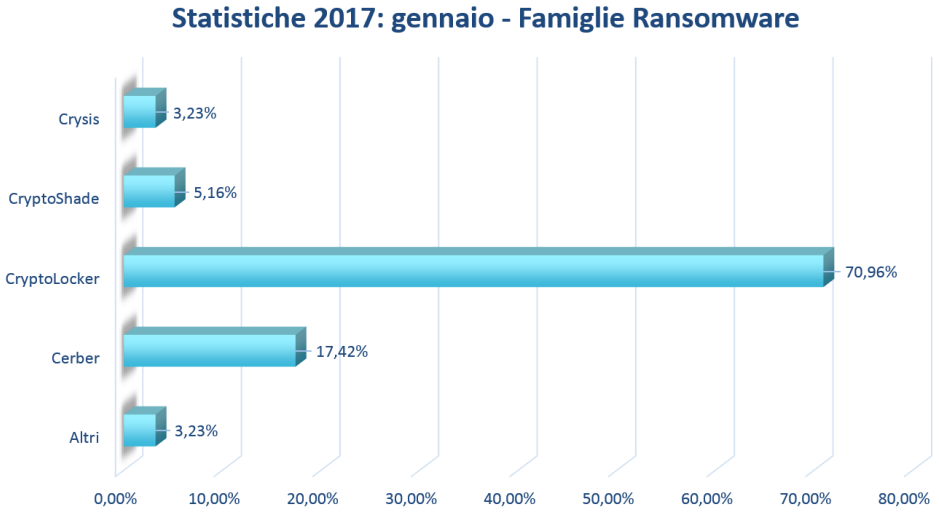
posizione. In questo mese fa la sua apparizione CryptoXXX, quasi un passaggio di testimone con TeslaCrypt. A maggio TeslaCrypt annuncia la chiusura del progetto ed in prima posizione si attesta CryptoXXX (60,54%), seguito da CryptoLocker (27,02%). A giugno si riconferma CryptoXXX (55,78%) seguito da CryptoLocker (22,45%).

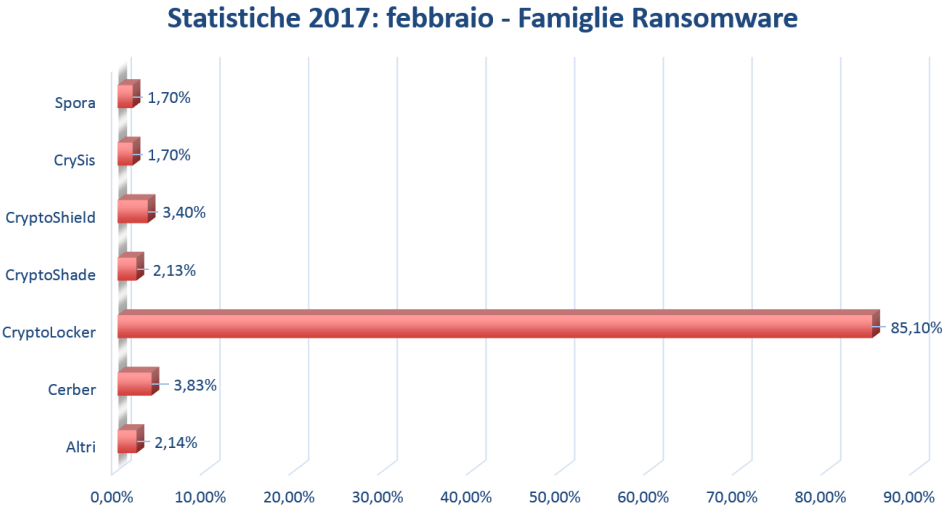


A luglio vi è una flessione del CryptoXXX (10,53%) che si trasforma in CryptoPPP, che gli costa però la prima posizione a favore di CryptoLocker (39,36%) e la seconda a favore di Locky (22,37%). Ad agosto il CryptoLocker (4,76%) va in ferie e il CryptoPPP (49,98%) balza in vetta superando il Locky (42,86%). A settembre CryptoLocker (34,04%), tornato dalle ferie, si riprende la prima posizione, seguito da Locky (20,21%) e da CryptoPPP (18,09%). A ottobre vi è una flessione delle infezioni da ransomware, in prima posizione troviamo Cerber (46,66%) seguito da Locky (26,66%), esce di classifica CryptoPPP. A novembre e dicembre la parte del leone la fa il CryptoLocker, seguito da Cerber e Locky.

Statistiche 2017

Per il 2017 possiamo avere un'anteprima dei primi 2 mesi, anche se i dati sono ancora parziali e quindi non definitivi, CryptoLocker è stato il ransomware con maggiore diffusione tra gennaio (70,96%) e febbraio (85,10%).





Quanto guadagnano i ransomware?

E' ragionevole chiedersi quanto possono aver guadagnato gli autori dei ransomware dai riscatti delle vittime. Rispondere a questa domanda con precisione non è però così facile. In rete è possibile trovare delle stime del possibile guadagno. Questi valori sono solamente stimati in base ad un ipotetico numero di infezioni moltiplicato per il riscatto richiesto, in questo modo gli analisti forniscono delle cifre ipotetiche.

Per conoscere realmente la cifra sborsata dalle vittime, bisognerebbe conoscere tutti i conti correnti in bitcoin (portafogli), dove le vittime hanno versato il riscatto. Ad esempio il CryptoLocker assegna ad ogni vittima un portafoglio distinto dove pagare la somma richiesta del riscatto. Non tutte le vittime pagano il riscatto e così non è possibile fare una stima esatta del possibile guadagno ottenuto dagli autori del ransomware.

Altri ransomware, come il CrySis, forniscono per un periodo limitato un unico portafoglio dove versare il riscatto. Analizzando alcune campagne delle famiglia CrySis siamo riusciti ad ottenere alcuni valori reali di incasso.

Data	Campagna	Wallet	Bitcoin
29-11-2016 15-12-2016	stopper	1FwHxzFFGbAmmdkxhUUTEjocuDhEowDyuU	67.56167621
29-11-2016 20-12-2016	worm01	1KQhTbj9sGrQ596wBPZLQTpbiN1gBXwAny	28.53519378
10-12-2016 15-12-2016	mkgoro	1swAqc6dAyqcSaKdx8VnuJhhE9vaYLHFb	8.09468500
12-12-2016 15-12-2016	payforhelp	1GKpUP4SWC7TiiX7BkeST4i9bFNVyyPTjb	4.00000000
13-12-2016 16-12-2016	bitcoin143	19PuzW2WwD4jnhQLLvHun7cCeJq8HZux4	9.00000000
20-12-2016 21-12-2016	amagnus	1DaeQHLUbckx2tnshQrmcE45tEMB1UxjPS	4.00000000
07-01-2017 11-01-2017	bitcoin143	1AJa5kZY1LDzSLrYJ3SDq3CubX8qHwpjEN	12.50000000
05-01-2017 16-01-2017	cryptsvc	116CZ4y4mHs9ruzmYCufrwk4t17dsNEnAJ	26.00070000
		Totale Bitcoin	159.69225499

1FwHxzFFGbAmmdkxhUUTEjocuDhEowDyuU

Total Received: 67.56167621

Total Sent: 50.49986950

Final Balance: 17.06180671

Total transactions: 30

Recent transactions:

Date ▼	Amount	Balance
2016-12-15 19:57:42	3.92000000	17.06180671
2016-12-15 15:43:01	1.00000000	13.14180671
2016-12-14 18:35:29	2.50000000	12.14180671
2016-12-14 17:20:43	4.00000000	9.64180671
2016-12-14 00:22:05	5.00180671	5.64180671
2016-12-13 11:48:17	0.64000000	0.64000000
2016-12-12 16:24:17	-14.49986950	0.00000000
2016-12-12 14:54:59	1.00000000	14.49986950
2016-12-12 05:38:55	1.00000000	13.49986950
2016-12-11 13:37:09	-3.00000000	12.49986950
2016-12-11 13:08:28	0.99986950	15.49986950
2016-12-11 07:49:25	1.00000000	14.50000000
2016-12-10 15:30:55	3.00000000	13.50000000
2016-12-10 03:07:32	3.00000000	10.50000000
2016-12-09 18:17:03	2.00000000	7.50000000
2016-12-07 22:47:53	2.50000000	5.50000000
2016-12-07 13:22:38	3.00000000	3.00000000
2016-12-06 16:59:53	-4.00000000	0.00000000
2016-12-05 18:40:50	4.00000000	4.00000000
2016-12-05 16:03:45	-21.00000000	0.00000000
2016-12-05 11:36:50	2.00000000	21.00000000
2016-12-03 12:11:09	3.00000000	19.00000000
2016-12-02 15:53:42	-8.00000000	16.00000000
2016-12-02 11:57:12	4.00000000	24.00000000
2016-12-02 05:21:39	4.00000000	20.00000000
2016-12-02 00:24:30	3.00000000	16.00000000
2016-12-01 21:45:28	4.00000000	13.00000000
2016-12-01 19:02:30	4.00000000	9.00000000
2016-12-01 17:00:59	1.00000000	5.00000000
2016-11-29 15:40:01	4.00000000	4.00000000

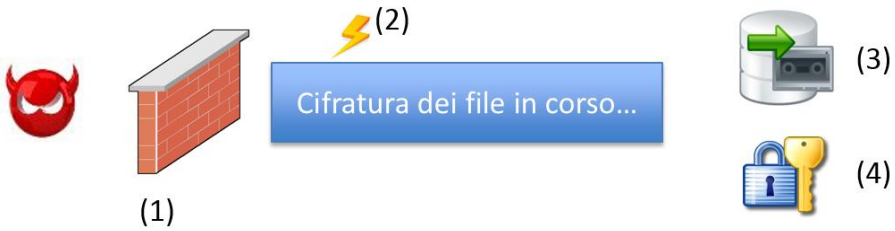
Dal 29 novembre 2016 al 16 gennaio 2017, le campagne del CrySis che abbiamo monitorato hanno incassato circa 159,70 BTC in un mese e mezzo.

Il 29 novembre 2016 1 BTC valeva 729.60 USD ed è sempre cresciuto superando quota 1000 $ a fine anno. Gli autori del CrySis hanno incassato più di 125.000,00 $ in un mese e mezzo.

In figura a sinistra possiamo vedere le transazioni del portafoglio relativa alla campagna “stopper”.

Come mi difendo

Dopo aver analizzato in profondità i vettori di diffusione, il funzionamento del ransomware e le loro statistiche in Italia, vediamo ora come possiamo difenderci da un attacco Crypto-Malware.



L'uso dell'antivirus "classico" e/o in abbinata a policy ci permette, in qualche modo di intercettare il malware prima che questo arrivi sul computer oppure di bloccarlo all'atto dell'esecuzione (1), a patto che l'antivirus riconosca il malware attraverso le "signature". In base alla tipologia del vettore d'infezione utilizzato, il software antivirus può intercettare il ransomware prima che questo arrivi fisicamente sul computer della vittima, attraverso queste tecnologie:

- WebFilter
- Policy allegati di posta elettronica
- Scudo in tempo reale

La tecnologia "WebFilter" permette al software antivirus di analizzare gli URL malevoli, in modo da bloccare l'accesso a questi siti e il conseguente download del software dannoso. L'uso di policy per gli allegati dei messaggi della posta elettronica, permette di bloccare file con estensione di tipo eseguibile come: .exe, .vbs, .js, .etc. Molti malware hanno iniziato ad utilizzare altre tipologie di allegato, come file .ZIP che possono contenere al loro interno file eseguibili, oppure file .DOC di Word o .XLS di Excel che contengono macro virus per scaricare malware o ancora file vettoriali di tipo .SVG che possono contenere codice javascript per il download di file malevoli. L'uso di policy nei file allegati potrebbe ridurre il rischio

d'infezione da ransomware. L'ultima nostra barriera prima che il ransomware venga eseguito è lo scudo in tempo reale che può intercettare il malware attraverso firme o cloud.

E' nell'interesse degli autori dei Crypto-Malware rilasciare in continuazione nuove varianti, in modo da by-passare i controlli degli antivirus. Gli autori dei ransomware si avvalgono di exploit kit, che sfruttano la tecnologia DGA (domain generation algorithm) per generare periodicamente nuovi domini e bypassare il controllo delle tecnologie WebFilter per l'analisi degli URL malevoli. Inoltre re-impacchettano il ransomware con packer proprietari o "custom" in modo da by-passare l'identificazione da parte degli anti-virus.

Capita spesso che il ransomware riesca ad arrivare sul computer della vittima. Anche se il crypto-malware è stato eseguito sul computer (2), ci possiamo avvalere di tecnologie anti-ransomware per mitigare la cifratura dei file. Gli anti-ransomware usano tecnologie pro-attive anti-crypto malware che vanno a mitigare l'attacco, bloccando il processo malevolo durante la cifratura dei file. Più veloce sarà la procedura anti-ransomware a reagire contro il malware, maggiore sarà la sua mitigazione, riducendo a qualche decina il numero dei file cifrati.

Se non disponiamo di tecnologie anti-ransomware e se il crypto-malware ha cifrato tutti i nostri file di documenti, possiamo recuperarli attraverso copie di backup (3), a patto che queste non siano state a loro volta cifrate.

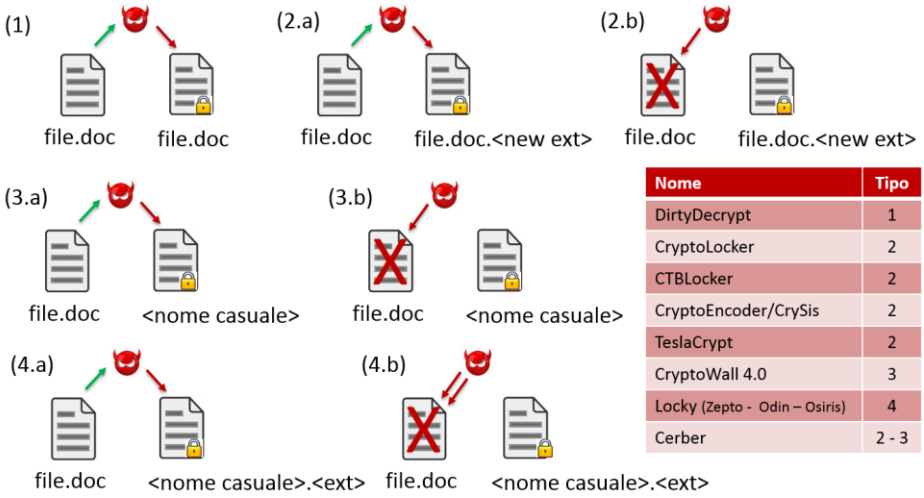
Se non si dovesse disporre di copie di backup oppure queste siano state cifrate, si potrebbe provare a recuperare i file (4), ad esempio decifrando i file criptati attraverso specifici tool realizzati ad hoc ove possibile, ma alcuni malware sono impossibili da decifrare senza conoscere la chiave di cifratura utilizzata, oppure attraverso tool di recupero dati di file cancellati.

Mitigazione dell'attacco: protezione Anti-Ransomware

La mitigazione dell'attacco attraverso un sistema anti-ransomware, si basa su un approccio euristico comportamentale, dove viene analizzato il comportamento di ogni singolo processo. Se un processo eseguirà operazioni atte alla cifratura di file, il sistema lo bloccherà inibendo l'accesso al file system. Il processo malevolo, continuerà a lavorare, ma non avendo più accesso al file system non potrà quindi cifrare ulteriori file di documento. Una caratteristica importante nella mitigazione dell'attacco è la disattivazione automatica delle connessioni di rete, in modo da bloccare i thread malevoli durante la cifratura di cartelle condivise.

I ransomware possono usare diversi schemi "comportamentali" per cifrare i file indipendentemente dall'algoritmo di criptazione utilizzato. Alcune tecnologie anti-ransomware analizzano le API del processo, altri sistemi utilizzano un approccio più a basso a livello analizzando il comportamento del processo.

Vediamo ora alcuni schemi comportamentali usati da alcune famiglie di ransomware durante le operazioni di cifrature.



Nome	Tipo
DirtyDecrypt	1
CryptoLocker	2
CTBLocker	2
CryptoEncoder/CrySis	2
TeslaCrypt	2
CryptoWall 4.0	3
Locky (Zepto - Odin – Osiris)	4
Cerber	2 - 3

Nello schema (1) il ransomware legge in memoria il file originale, il buffer in memoria viene cifrato e dopo riscritto nel file originale. La vittima si troverà il file con il nome originale, ma col contenuto cifrato. Nello schema (2.a) il ransomware legge in memoria il file originale, il buffer in memoria viene cifrato e dopo scritto in un nuovo file, avente come nome il file originale ma con una nuova estensione. Nella fase (2.b) il file originale viene cancellato, così la vittima si troverà ad avere file cifrati del tipo "file.doc.<new ext>". Nello schema (3.a) e (3.b) il nuovo file creato ha un nome completamente casuale non riconducibile al file originale.
Nell'ultimo schema (4.a) e (4.b) il nuovo file creato ha un nome casuale ma un'estensione "costante" del ransomware e il file originale prima di essere cancellato viene sovrascritto con valori casuali.

Questi sono solo alcuni schemi comportamentali utilizzati dai ransomware, ad esempio lo schema 2 è adottato da CryptoLocker, CTBLocker o TeslaCrypt, lo schema 3 da CryptoWall e lo schema 4 da Locky. Il Cerber ha adottato più schemi comportamentali passando dal 2 al 3.

La guerra tra ransomware e tecnologie anti-ransomware è come una partita a scacchi con mosse e contro-mosse per sconfiggere l'avversario e aggiudicarsi la vittoria di una battaglia. Chi vincerà la guerra?

VirIT protezione Anti-Ransomware

A partire da maggio 2015 nell'antivirus VirIT eXplorer PRO è stata implementata la protezione anti-ransomware per mitigare questa tipologia di attacco, in modo da salvaguardare i file di documenti dalla cifratura.

La protezione anti-crypto malware di VirIT monitora una serie di tipologie di documenti (doc, xls, pdf, jpg, etc.) nel caso che questi file dovessero venire cifrati. Quando il numero di file cifrati raggiunge la soglia massima, il sistema anti-ransomware interviene inibendo l'accesso ai file al processo malevolo.

Per migliorare la mitigazione dell'attacco è stato implementato un sistema di "backup on-the-fly", che esegue un backup al volo dei file di documento di dimensione compresa tra i 2 KB e i 3MB in fase di cancellazione o troncamento del file. Questo è un plus che permette a VirIT di recuperare in molti casi i file "sacrificati" durante la fase iniziale dell'attacco.

Quando entra in funzione la protezione anti-ransomware, VirIT disattiva automaticamente le connessione di rete LAN, questo permette di mitigare l'attacco sulle cartelle condivise degli altri computer.

Per ultimo, VirIT è in grado proteggere il computer anche se l'attacco avviene da un computer esterno sulla cartella locale condivisa.

Nell'esempio illustrato, solo un pc è difeso da VirIT. Se un computer della rete venisse colpito da ransomware, questo cifrerà tutti i documenti locali e delle cartelle condivise degli altri pc. Cosa succederà nel computer protetto da VirIT? Nel PC protetto da VirIT, l'attacco sarà mitigato dalla protezione anti-ransomware inibendo l'accesso al file system al processo denominato "system", poiché l'attacco è avvenuto dall'esterno e non da un processo locale.

La protezione anti-ransomware di VirIT è in grado di mitigare l'attacco dalla maggior parte dei ransomware in circolazione, anche di nuova generazione. Per alcune particolari tipologie, come TeslaCrypt, è stato implementato la possibilità di carpire la chiave privata utilizzata dal malware durante la cifratura, questo permette di recuperare tutti i file cifrati da questo ransomware.

Nome	Prot. Anti-Crypto Malware	Backup on-the-fly	Recupero Chiave privata
CryptoLocker	Si	Si	-
CTBLocker	Si	Si	-
CryptoWall 3.0	Si	Si	-
TeslaCrypt (1.0, 2.0, 3.0, 4.0)	Si	No	Si
CryptoEncoder/CrySis	Si	Si	-
CryptoFF	Si	No	Si
CryptoWall 4.0	Si	Si	-
Cerber	Si	No	-
Locky – Zepto - Odin	Si	No	-
HydraCrypt (CryptoXXX)	Si	No	-
DMA Locker	Si	No	-
Sage	Si	Si	-
Mischa	Si	No	-
CryptoPPP	Si	Si	-
CryptoShield	Si	Si	-
Petya	No	-	-

E' possibile vedere l'efficacia della tecnologia anti-ransomware di VirIT nella simulazione di un attacco da TeslaCrypt 3.0 su macchina virtuale, video su youtube: https://youtu.be/_SyKqqZu6-8

In base alle statistiche di Ottobre 2015, l'efficacia della tecnologia anti-ransomware integrata in VirIT è pari al 99,63 %, che rappresenta l'aspettativa percentuale media dei file salvati dalla cifratura da VirIT.

Statistica Ottobre 2015	
Media dei file crittografati su PC / SERVER con la protezione Anti-CryptoMalware integrata in Vir.IT eXplorer PRO	157
Media dei file crittografati con Anti Virus-Malware diverso da Vir.IT	42.452
Efficacia della tecnologia Anti-CryptoMalware integrata in Vir.IT eXplorer PRO	**99,63%***

* Aspettativa percentuale media di file salvati dalla cifratura grazie alla protezione anti-ransomware di Vir.IT eXplorer PRO: https://www.tgsoft.it/italy/news_archivio.asp?id=664

Backup

Il Backup è l'unica soluzione che permette di recuperare i file cifrati da un attacco da crypto-malware. E' bene ricordare, che le copie di backup, devono essere scollegate dalla rete, per non incorrere nelle cifratura delle stesse ed è consigliabile sempre tenere più copie di backup.
E' possibile utilizzare soluzioni di backup in cloud, ma è importante sottolineare il problema della sincronizzazione, ad esempio DropBox, nel caso di cifratura dei file locali. In questo caso, DropBox eseguirà la sincronizzazione dei file cifrati, andando a sostituire i file buoni con quelli cifrati, quindi è cosa buona tenere uno storico dei backup.

Anche in VirIT è stato integrato la funzionalità di Backup, da non confondersi con il "backup on-the-fly", trattasi di un modulo denominato "VirIT Backup", ove le copie di backup saranno protette dalla scrittura da VirIT e quindi non potranno essere cifrate o cancellate da malware.

Vi sono alcuni punti di criticità tipici di qualsiasi sistema di Backup:

- tempo/lavoro per eseguire il backup o il ripristino dei dati
- copie obsolete

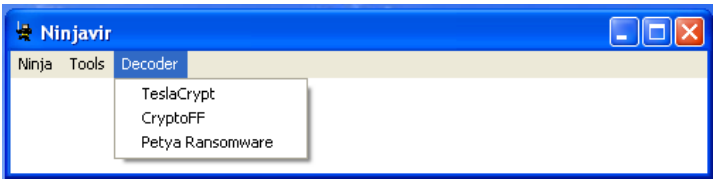
E' possibile recuperare i file cifrati?

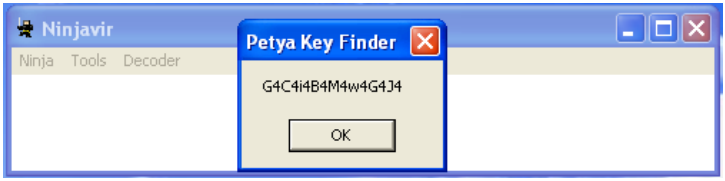
Se non disponiamo di copie di backup oppure queste sono state cifrate, vi sono poche possibilità di recuperare i file se questi sono stati cifrati con algoritmi come AES, RSA o Salsa20, a meno che non si conosca la chiave di cifratura utilizzata.

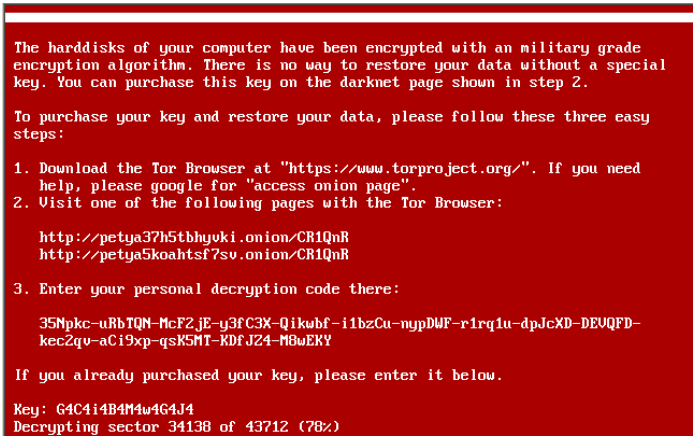
In passato sono state recuperate chiavi private da server di C&C sequestrati dalle forze dell'ordine. In altri casi, gli autori dei crypto-malware hanno commesso degli errori e hanno lasciato dei punti deboli, come nel caso TeslaCrypt (versioni precedenti alla 3.0) o nelle prime release di Petya.

Nel caso di Petya, un'errata implementazione di Salsa20 e la sovrascrittura parziale della chiave di cifratura ha permesso il calcolo della chiave utilizzata.

Il C.R.A.M. di TG Soft ha realizzato un tool per decifrare la prima versione di Petya, integrato nel modulo Ninjavir.







In altri casi è possibile determinare la chiave di cifratura ipotizzando la chiave casuale utilizzata, alcuni ransomware utilizzano la chiave casuale ottenuta dalla funzione random: rnd (time()).

Nel campo della cifratura la funzione random *rnd()* non è consigliata per la generazione di chiavi casuali. La funzione rnd(time()) utilizza come seme

l'API *time(),* la quale restituisce data e ora del computer all'atto della chiamata. Dai file cifrati è possibile determinare data e ora di modifica, applicando tali valori come seme alla funzione rnd() è possibile determinare la chiave di cifratura utilizzata.

In alcuni casi è possibile applicare il brute force per ottenere la chiave utilizzata, in questo caso è necessario avere il file cifrato e il file originale per determinare la chiave. Le chance per ottenere la chiave di cifratura con il brute force dipendono però dalla lunghezza delle chiavi utilizzate.

Ad ogni modo se il ransomware utilizza correttamente gli algoritmi di cifratura come AES, RSA o Salsa20, e la chiave di cifratura è calcolata con la funzione CryptGenRandom, non è possibile decifrare i file senza conoscere la chiave utilizzata.

In alcuni casi è possibile recuperare i file cifrati dalle "shadow copies" con *Shadow Explorer*. Molti ransomware prima di iniziare a cifrare i file, cancellano le shadow copies, rendendone impossibile il recupero.

Con l'UAC (User Account Control) attivo, la cancellazione delle "shadow copies" necessitano dell'autorizzazione da parte dell'utente. Inoltre alcuni ransomware si limitano a cancellare le "shadow copies" solo dall'unità "C:", permettendo così il recupero delle "shadow copies" dalle altre unità.

Come ultima possibilità, possiamo ricorrere al recupero dei file attraverso tool di recovery ("file carver"), che ripristinano file "accidentalmente" cancellati, come ad esempio Recuva o PhotoRec.

Il caso TeslaCrypt

Per le versioni precedenti alla 3.0 di TeslaCrypt è possibile recuperare i file con i tool: TeslaDecoder (*BloodDolly*), TeslaCrack (*Googulator*) e The Talos TeslaCrypt Decryption Tool (*Cisco*).

Il punto debole delle versioni precedenti alla 3.0 è stato quello di aver reso disponibile il valore *session_ecdh_secret_mul*:

session_ecdh_secret_mul = session_ecdh_secret * session_chiave_privata

A questo punto ci viene in aiuto "*Il teorema fondamentale dell'aritmetica*" che afferma:

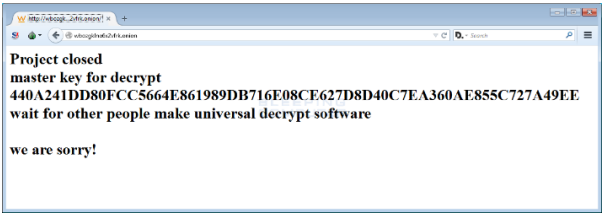
"*Ogni numero naturale maggiore di 1 o è un numero primo o si può esprimere come prodotto di numeri primi. Tale rappresentazione è unica, se si prescinde dall'ordine in cui compaiono i fattori*."

$$n=p\_1*p\_2*...*p\_k$$

Attraverso la fattorizzazione è stato possibile determinare la chiave privata di session_chiave_privata fattorizzando il valore session_ecdh_secret_mul.

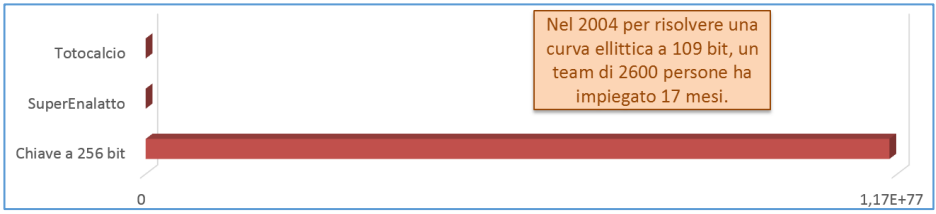
Dalla versione 3.0 del TeslaCrypt, non è più stato possibile decifrare i file senza conoscere la chiave privata. La chiave privata del TeslaCrypt è un numero casuale di 256 bit e la chiave pubblica è un punto della curva ellittica *secp256k1*.

Fortunatamente gli autori del TeslaCrypt hanno chiuso il progetto e hanno rilasciato pubblicamente la chiave privata master utilizzata per la cifratura, permettendo la decifratura di qualunque file del TeslaCrypt.



Per capire quanto sia complesso individuare la chiave privata attraverso un attacco "brute force", abbiamo calcolato il numero di combinazioni di alcuni giochi e della chiave a 256 bit:

- Totocalcio (13 partite) = 3^{13} = 1.594.323
- SuperEnalotto = C(90,6) = 622.614.630 (388 volte quelle del totocalcio)
- Per le chiavi a 256 bit ci vogliono 1,16 * 10^{77} combinazioni.



Se raffrontiamo graficamente questi 3 dati, vediamo che è molto più facile vincere al Totocalcio o al SuperEnalotto che individuare una chiave privata a 256 bit.

Rapporto aggiornato a febbraio 2017

Nella convinzione che questo rapporto sui Ransomware in Italia sia stato trovato interessante e abbia fornito a tutti coloro che l'abbiano letto con la dovuta attenzione conoscenze e spunti tecnici, non ci resta che lasciarvi con un ARRIVEDERCI al prossimo aggiornamento…

Gianfranco Tonello

Ransomware 2017

Italy

Gianfranco **Tonello**

TG Soft
Security Software Specialist
ANTIVIRUS · ANTISPYWARE · ANTIMALWARE
www.tgsoft.it

C.R.A.M.
CENTRO RICERCHE ANTI-MALWARE