

**smau**

**PADOVA 10-11 MARZO 2016**

# Scacco matto ai Crypto-Malware!



PadovaFiereSpa

Come mettere al sicuro i nostri dati più preziosi.



Ing. Gianfranco Tonello

# Scacco matto ai Crypto-malware!



## Ransomware: cosa sono ?

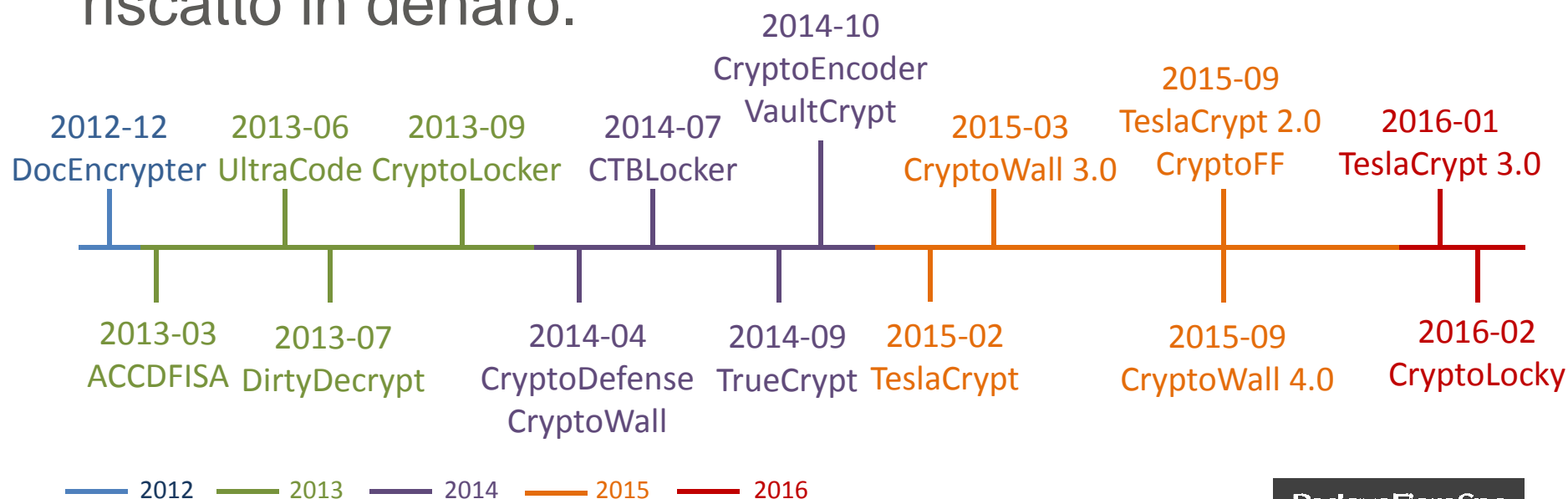
Con il termine **Ransomware** definiamo tutti quei programmi o software che bloccano l'accesso ai file di documenti o al computer chiedendo un riscatto in denaro per accedervi.

Esempi di Ransomware:

- Trojan.Win32.FakeGdF
- Crypto-Malware

# Crypto-Malware: cosa sono ?

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

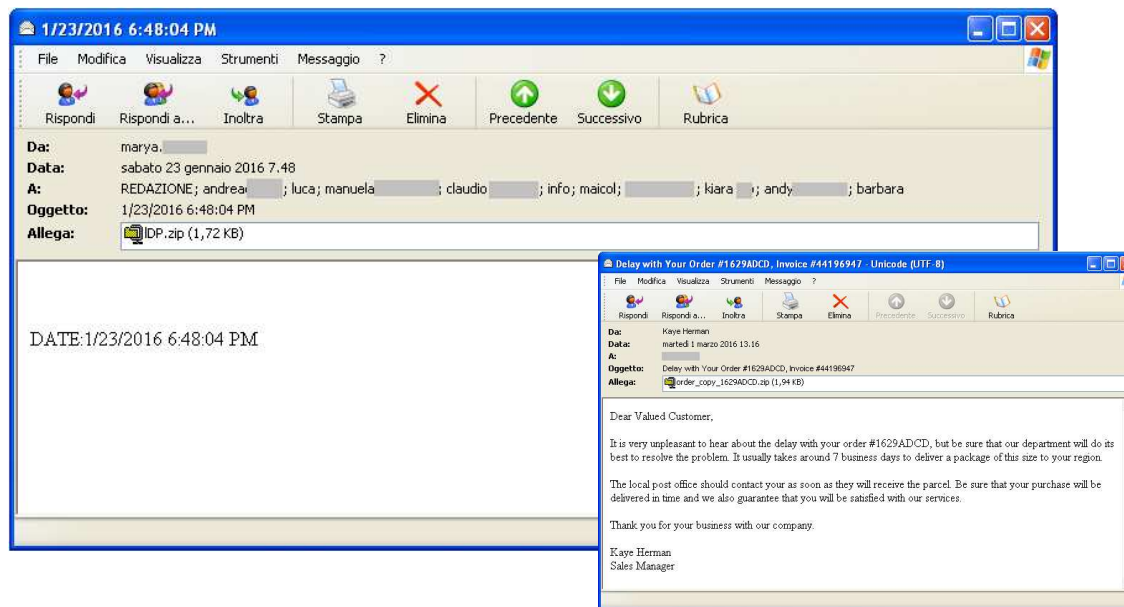


# Metodo di diffusione

- via email (ingegneria sociale)
- drive-by-download
- siti infettati (utilizzo di vulnerabilità)
- altri malware

## TeslaCrypt 3.0

- 4000 account SMTP compromessi
- 45 milioni di indirizzi email





# CryptoLocker - TorrentLocker

- anno: 2013 settembre
- estensione: .encrypted
- algoritmo: AES
- riscatto: 300/600 euro (in bitcoin)
- rete: Tor-Onion



Nome	Ultima modifica	Tipo	Dimensione
COME_RIPRISTINARE_I_FILE	02/03/2016 13:57	Chrome HTML Do...	9 KB
COME_RIPRISTINARE_I_FILE	02/03/2016 13:57	Documento di testo	4 KB
DSC0191.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.486 KB
DSC0191.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.523 KB
DSC0193.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.498 KB
DSC0194.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.508 KB
DSC0195.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.476 KB
DSC0196.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.457 KB
DSC0197.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.544 KB
DSC0198.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.521 KB
DSC0199.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.471 KB
DSC0200.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.564 KB
DSC0201.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.517 KB
DSC0202.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.572 KB
DSC0203.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.546 KB
DSC0204.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.497 KB
DSC0205.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	6.377 KB
DSC0206.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	3.486 KB
DSC0207.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	3.338 KB
DSC0208.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	3.520 KB
DSC0209.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	3.516 KB
DSC0210.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	3.508 KB
DSC0211.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	3.482 KB
DSC0212.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	3.429 KB
DSC0213.JPG.encrypted	02/03/2016 13:57	File ENCRYPTED	3.413 KB

**ATTENZIONE**

**abbiamo criptato i vostri file con il virus CryptoLocker**

I vostri file importanti (compresi quelli sui dischi di rete, USB, ecc): foto, video, documenti, ecc sono stati criptati con il nostro virus CryptoLocker. L'unico modo per ripristinare i file è quello di pagare noi. In caso contrario, i file verranno persi.

Attenzione: La rimozione di CryptoLocker non ripristinare l'accesso ai file criptati.

[Clicca qui per pagare per i file di recupero](#)

**Domande frequenti**

**[+] Che cosa è successo ai miei file?**  
Capire il problema

**[+] Come faccio a ripristinare i miei file?**  
L'unico modo per ripristinare i file

**[+] Cosa devo fare dopo?**  
Acquista decrittazione

**[+] Non riesco ad accedere al tuo sito web, cosa devo fare?**  
Accesso specchi sito web utilizzando

**Acquista decrittazione e ripristinare i file**

Acquista decrittazione per **299 EUR** prima 2016-03-09 12:19:32  
 O acquistare in un secondo momento con il prezzo di **598 EUR**  
 Tempo rimasto prima di aumento del prezzo: **49:15:24**  
 Numero di file criptati: 166

Prezzo corrente: **0.8187816 Bitcoin** (circa 299 EUR)  
 Pagato: **0 Bitcoin** (circa 0 EUR)  
 Rimanendo a pagare: **0.8187816 Bitcoin** (circa 299 EUR)

**Acquista decifratura con Bitcoin**

Cosa sono i Bitcoin?  
 Bitcoin (simbolo: B; codice: BTC o XBT) è una moneta elettronica.

**1. Acquista bitcoin**

Quando si acquista bitcoin, non dire il venditore che si sta pagando per il file di decrittazione. Diciamo che si sta acquistando Bitcoin come un investimento. Nel solo un modo per ottenere il vostro file indietro - nel pagare l'importo richiesto in bitcoin. La polizia solo figure di lavoro, non hanno alcuna possibilità di aiutare.

Si prega di consultare consigliato bitcoin venditori nel tuo paese:  
[www.bitcoin.it](http://www.bitcoin.it) - Compra Bitcoin con Postepay/Bonifico Bancario  
[www.bitfiddle.it](http://www.bitfiddle.it) - Compra Bitcoin con Postepay/Bonifico Bancario  
[www.bitstamp.net](http://www.bitstamp.net) - Il mercato numero uno in Italia, per comprare Bitcoin istantaneamente, in contanti.  
[postbit.it](http://postbit.it) - Compra bitcoin in contanti senza registrazione!  
[www.mars78.biz](http://www.mars78.biz) - Compra Bitcoin con Postepay, SuperFlash,  
[www.baypaycoins.com](http://www.baypaycoins.com) - Compra Bitcoin con Mybank, Sofort,  
[www.bitbit.com](http://www.bitbit.com) - Compra Bitcoin con Postepay, Sepa, Sofort,  
[localbitcoins.com](http://localbitcoins.com) - Compra bitcoin online in Italy  
[howtobuybitcoins.info](http://howtobuybitcoins.info) - Come acquistare bitcoin in Italia.

**2. Invia bitcoin**



# CTBLocker: Curve Tor Bitcoin Locker

- anno: 2014 luglio
- estensione: .<casuale di 7 char>
- algoritmo: AES
- riscatto: 2 BTC
- rete: Tor-Onion

**I tuoi dati personali sono criptati da CTB-Locker.**

**I tuoi dati personali sono criptati da CTB-Locker.**

I tuoi documenti, foto, dati e altri file importanti sono stati criptati con la crittografia forte e chiave univoca, generati per questo computer.

Chiave privata di decodifica e' memorizzata su un server segreto e nessuno puo' decifrare i file fino a quando si paga per ottenere la chiave privata.

Hai solo 96 ore per fare il pagamento. Se non paghi entro il tempo previsto, tutti i file rimarranno cifrati per sempre e nessuno sarà in grado di recuperarli.

Premi 'Esamina' per visualizzare l'elenco dei file che sono stati criptati.

Premi 'Avanti' per la pagina prossima.

**ATTENZIONE! NON CERCARE DI SBARAZZARTI DEL PROGRAMMA DA SOLO. QUALSIASI AZIONE INTRAPRESA CONPORTERA' LA DISTRUZIONE DI TUTTI I FILE PER SEMPRE. L'UNICO MODO PER SALVARE I VOSTRI FILE E SEGUIRE LE ISTRUZIONI.**

Esamina **95:58:35** Avanti >>

E' possibile aprire e utilizzare copia-incolla per l'indirizzo e la chiave.

**I tuoi dati personali sono criptati da CTB-Locker.**

I tuoi documenti, foto, dati e altri file importanti sono stati criptati con la crittografia forte e chiave univoca, generati per questo computer.

Chiave privata di decodifica e' memorizzata su un server segreto e nessuno puo' decifrare i file fino a quando si paga per ottenere la chiave privata.

Se viene visualizzata la finestra principale di Loker, segui le istruzioni sul loker. Se non visualizzate nulla, sembra che voi o il vostro antivirus abbiate eliminato il programma loker. Ora avete l'ultima possibilita' di decifrare i file.

Apri <http://tmc2ybfqzkaeil.onion.cab> o <http://tmc2ybfqzkaeil.tor2web.org> nel tuo browser. Sono porte pubbliche al server segreto.

Se hai problemi con porte, utilizza la connessione diretta:

1. Scaricare Tor Browser dalla <http://torproject.org/>
2. Nel Browser Tor aprire la <http://tmc2ybfqzkaeil.onion/>.  
Si noti che questo server e' disponibile solo tramite Tor Browser. Riprova tra 1 ora se il sito non e' raggiungibile.

Scrivi nella seguente chiave pubblica nel form ingresso sul server. Evita errori di stampa.  
RYPPCBK-5LL65IY-B7MG6J2-TIQVYZV-GHN4BBG-RN3IJ2V-H6JQU3H-JYQNNRD  
2P8I5TD-UGSYORJ-DCQZ8TD-8EG2HX3-48VT4B4-5MH3G3M-ITVRARX-XUVBVXG  
QE23REW-QLZHBDE-HFJV2JU-5GW6L8N-BFR2IHO-L45L82-LCJCBH4-BWRN82P

Segui le istruzioni sul server.

Queste istruzioni sono anche salvate in file con nome Decrypt-All-Files.txt nella cartella Documenti.  
E' possibile aprire e utilizzare copia-incolla per l'indirizzo e la chiave.

**Payment required**

Server accepts payment in Bitcoin (BTC) only.

If you have bitcoins:

1. Pay amount of 2 BTC to address: **1PVkLv6oZQtz3x6cAxIQ8HG8A95eYfWVei**
2. Transaction will take about 15-30 minutes to confirm.

If you do not have bitcoins:

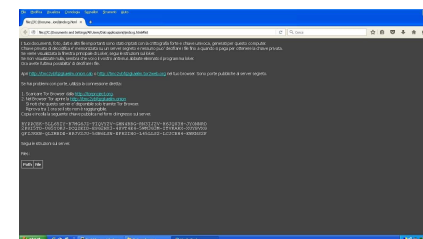
1. Open one of the exchangers:  
[https://en.bitcoin.it/wiki/Buying\\_bitcoins](https://en.bitcoin.it/wiki/Buying_bitcoins)  
<https://bitdirect.eu/>  
<https://www.bitboat.net/it/buy>  
<https://bitonic.nl/>
- and select exchange in your country and currency.  
Or open <https://localbitcoins.com/> and find person who sells bitcoins near you.

- Buy 2 BTC (about of 840 USD) and make direct deposit to bitcoin address: **1PVkLv6oZQtz3x6cAxIQ8HG8A95eYfWVei**
- Exact payment amount can vary depending of exchange rates.
- Transaction completion may take several days.

Reload this page in 15 minutes. After transaction completes you will be redirected to decryption page.  
Don't worry if some errors occurs and connection was broken. Wait 15 minutes and press F5.

To make sure that decryption is possible you are allowed to decrypt 2 any files for free. File size is limited up to 1 Mbyte.

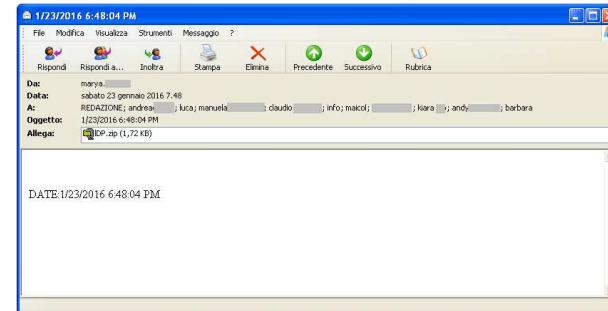
Encrypted file:  Nessun file selezionato.





# TeslaCrypt

- anno: 2015 febbraio
- estensioni: .micro, .mp3 (varie)
- algoritmo: AES
- riscatto: 500/1000 USD (in bitcoin)
- rete: Tor-Onion
- versione: 3.0



**Your files are encrypted.**  
 To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **08/03/16** the cost of decrypting files will increase **2 times** and will be **1000 USD**

Prior to increasing the amount left:  
**136h 59m 51s**

First connect IP: 93.61.119.77

Refresh Payment FAQ Decrypt 1 file for FREE Support

We give you the opportunity to decipher 1 file free of charge! You can make sure that the service really works and after payment for the CryptoWall program you can actually decrypt ALL files.

Please select a file to decrypt and upload it

Sfogliare... Nessun file selezionato. Upload file

Note: file should not be more than 512 kilobytes

Your files are encrypted.  
 To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **08/03/16** the cost of decrypting files will increase **2 times** and will be **1000 USD**

Prior to increasing the amount left:  
**137h 01m 01s**

First connect IP: 93.61.119.77

Refresh Payment FAQ Decrypt 1 file for FREE Support

We present a special software - CryptoWall Decrypter - which allows to decrypt and return control to all your encrypted files. [How to buy CryptoWall Decrypter?](#)

- You can make a payment with **Bitcoin**. There are many methods to get them.
- You should register **Bitcoin wallet** ([Bitcoin](#), [Bitcoin-Litecoin](#), [wallet](#) OR [some other methods of creation](#), [wallet](#))
- Purchasing **Bitcoin** - Although it's not yet easy to buy Bitcoins, it's getting simpler every day.

Here are our recommendations:

- [Bitcoin.eu](#) - Good service for Europe
- [Bitcoin.it](#) - Get BTC with Visa/MC or SEPA/EU Bank transfer
- [Bitcoin24.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you (Money/USD, Cash, BSN, Paypal and many others)
- [BTC24.com](#) - Buy Bitcoin with Visa/Mastercard or Wire Transfer
- [Bitcoin24.com](#) - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by Postfix, Moneygram, Money Order
- [Bitcoin24.com](#) - One and trusted Bitcoin dealer
- [Bitcoin24.com](#) - BTC dealer. Visit here and see...

Couldn't find BTC in your location? Try searching these directions:

- [bitcoin24.com](#) - An international directory of bitcoin exchanges.
- [Bitcoin24.com](#) - One more BTC dealer directory
- [Bitcoin24.com](#) - An international directory of bitcoin exchanges.
- [Bitcoin24.com](#) - EU countries directory.

Send 1.2 BTC to Bitcoin address: 16qjyMmVuz23kxWjy51dCu559Pbc6

Enter the Transaction ID and choose payment option:

Note: Transaction ID - you can find it in details info about transaction you made (example: 4c214648a5d6f39380a0523a3d54f18a21420785f63a2a08116441d)

Please check the payment information and click "PAY".

Num.	Diff. type	Your send drafts	Diff. number or transaction ID	Amount	Status
Your payments will be here.					

0 valid drafts are put, the total amount of 0 USD.

**NOT YOUR LANGUAGE? USE Google Translate**

**What happened to your files?**  
 All of your files were protected by a strong encryption with RSA4096  
 More information about the encryption RSA4096 can be found [https://en.wikipedia.org/wiki/RSA\\_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

**What does this mean?**  
 This means that the structure and data within your files have been irrevocably changed, you will not be able work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them

**How did this happen?**  
 Especially for you, our SERVER generated the secret key  
 All your files were encrypted with the public key, which has been transferred to your computer via the Internet.  
 Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program which is on our Secret Server!!

**What do I do?**  
 Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed  
 If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

- <http://s0ndr5344ygfwevjBfkwdHsefvHeliofeteH.at/B84FFD5A49673D3>
- <http://pts764g1354fder34fsqwd5gdfsavdftgfgkraskula.com/B84FFD5A49673D3>
- <http://yyre45dbyn2nbefbmbbegumvelic.at/B84FFD5A49673D3>

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

- Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
- After a successful installation, run the browser and wait for initialization.
- Type in the tor-browser address bar: [xlowfzng4w7dli.onion/B84FFD5A49673D3](http://xlowfzng4w7dli.onion/B84FFD5A49673D3)
- Follow the instructions on the site.

**!!! IMPORTANT INFORMATION:**

Your Personal PAGES:  
<http://s0ndr5344ygfwevjBfkwdHsefvHeliofeteH.at/B84FFD5A49673D3>  
<http://pts764g1354fder34fsqwd5gdfsavdftgfgkraskula.com/B84FFD5A49673D3>  
<http://yyre45dbyn2nbefbmbbegumvelic.at/B84FFD5A49673D3>  
 Your Personal TOR-Browser page : [xlowfzng4w7dli.onion/B84FFD5A49673D3](http://xlowfzng4w7dli.onion/B84FFD5A49673D3)  
 Your personal ID (if you open the site directly): B84FFD5A49673D3

# CryptoLocky

- anno: 2016 febbraio
- estensioni: .locky
- algoritmo: RSA - AES
- riscatto: 0,5 – 1 – 3 BTC
- rete: Tor-Onion

**!!! INFORMAZIONI IMPORTANTI!!!!**

Tutti i tuoi file sono stati criptati con algoritmo asimmetrico RSA-2048 e algoritmo simmetrico AES-128. Ulteriori informazioni sugli algoritmi sono disponibili su:

- http://it.wikipedia.org/wiki/RSA
- http://it.wikipedia.org/wiki/Advanced\_Encryption\_Standard

La decriptazione dei tuoi file è possibile solo con la chiave privata e il programma di decriptazione che si trova sul nostro server segreto.

Per ricevere la tua chiave privata vai a uno dei seguenti link:

1. <http://i3ezlvkoi7fwyood.tor2web.org/EF423B59EA8A7266>
2. <http://i3ezlvkoi7fwyood.onion.to/EF423B59EA8A7266>
3. <http://i3ezlvkoi7fwyood.onion.cab/EF423B59EA8A7266>

Se nessuno dei precedenti indirizzi è disponibile, segui i passaggi successivi:

1. Scarica e installa Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. Dopo la corretta installazione, avvia il browser e attendi l'inizializzazione.
3. Nella barra degli indirizzi digita: [i3ezlvkoi7fwyood.onion/EF423B59EA8A7266](http://i3ezlvkoi7fwyood.onion/EF423B59EA8A7266)
4. Segui le istruzioni a video.

!!! Il tuo numero d'identificazione personale è: EF423B59EA8A7266 !!!

### 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](#)
  - [bitvicious.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.

# Come funziona il CryptoMalware



email o sito infetto



esecuzione cryptomalware



invio/ricezione della chiave al/dal server C/C



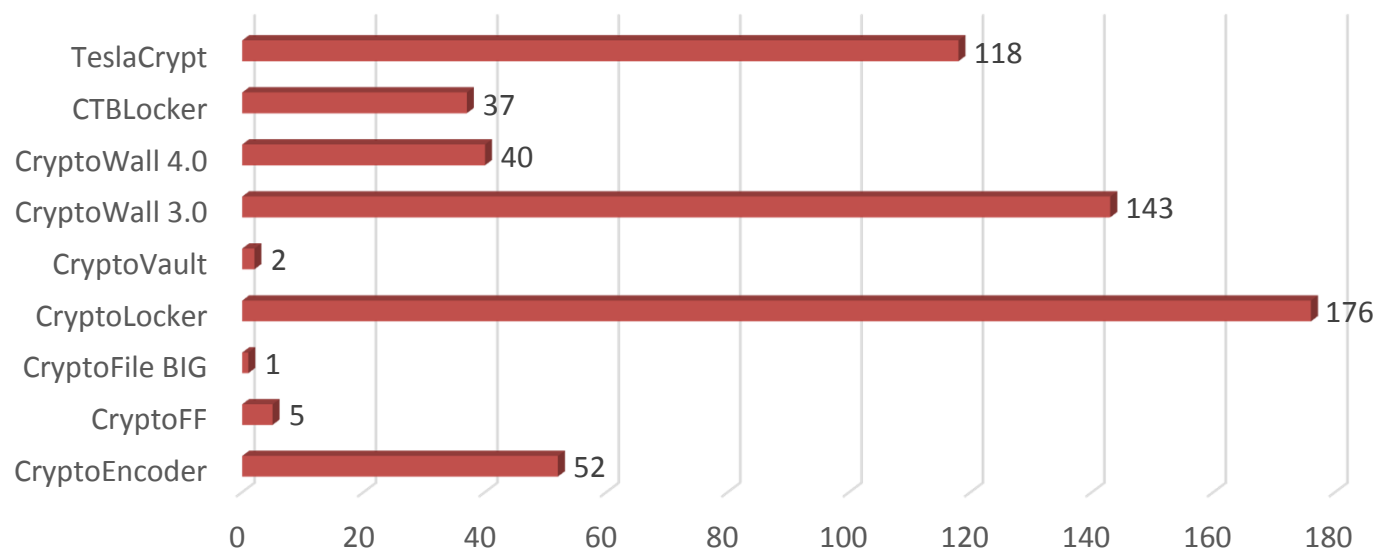
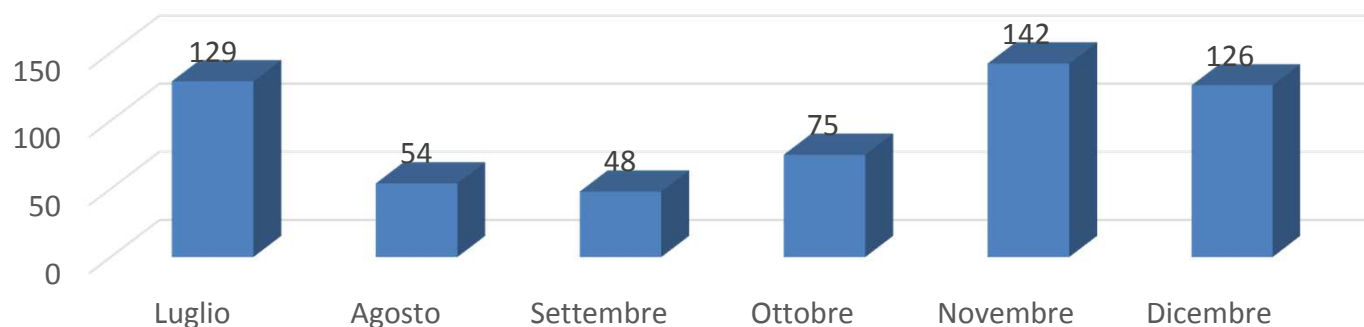
cifratura documenti locali e di rete



richiesta riscatto

# Statistiche: da Luglio a Dicembre 2015 (Italy)

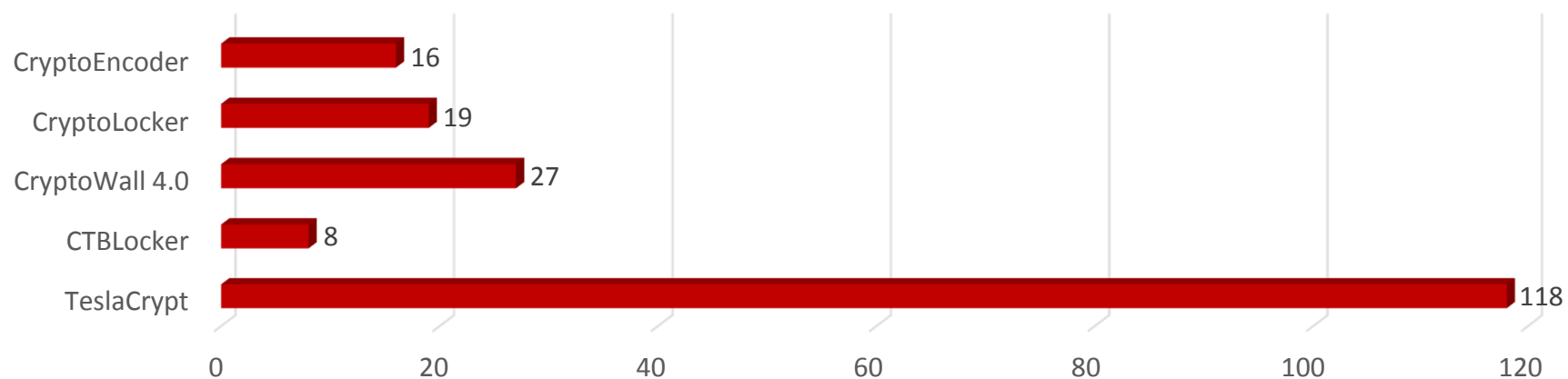
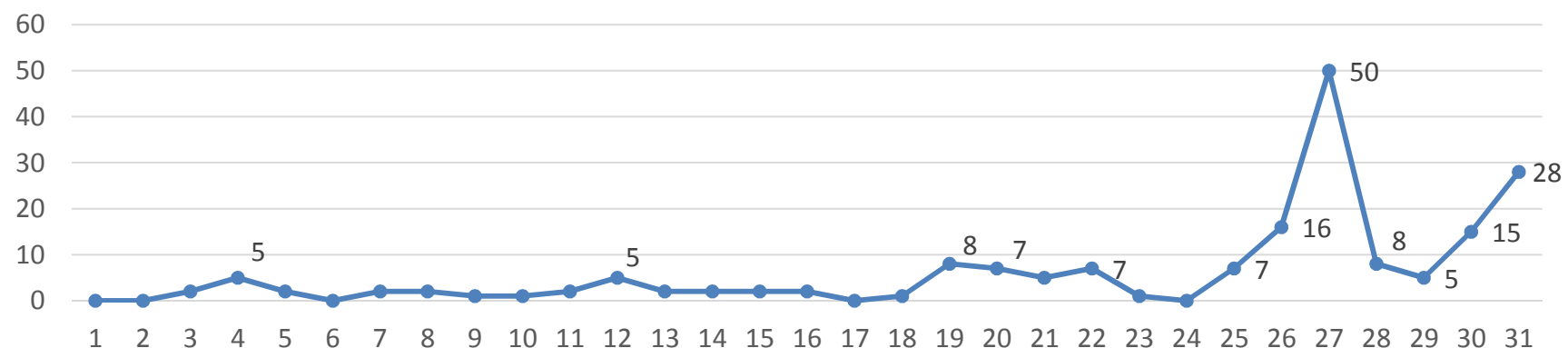
Numero di casi da Luglio a Dicembre 2015: 574



# Statistiche: Gennaio 2016 (Italy)

Num. casi: 188

Dist. temporale: num. casi al giorno

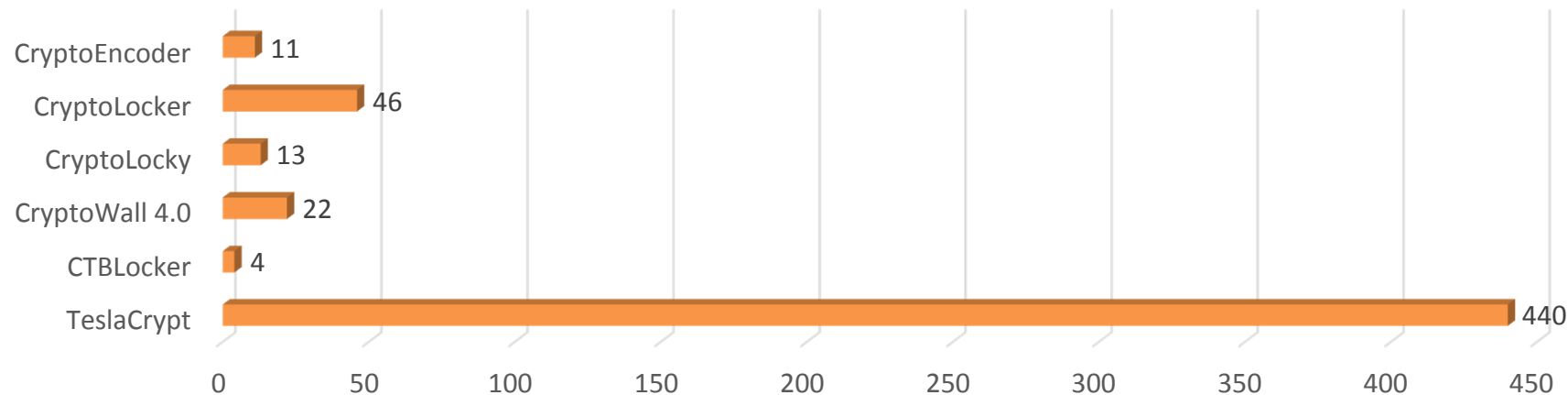
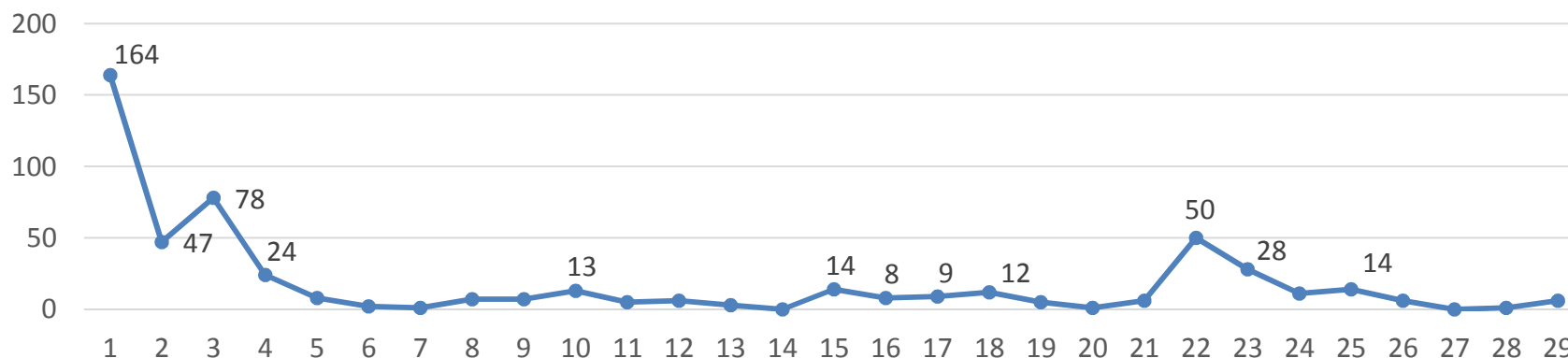




# Statistiche: Febbraio 2016 (Italy)

Num. casi: 536

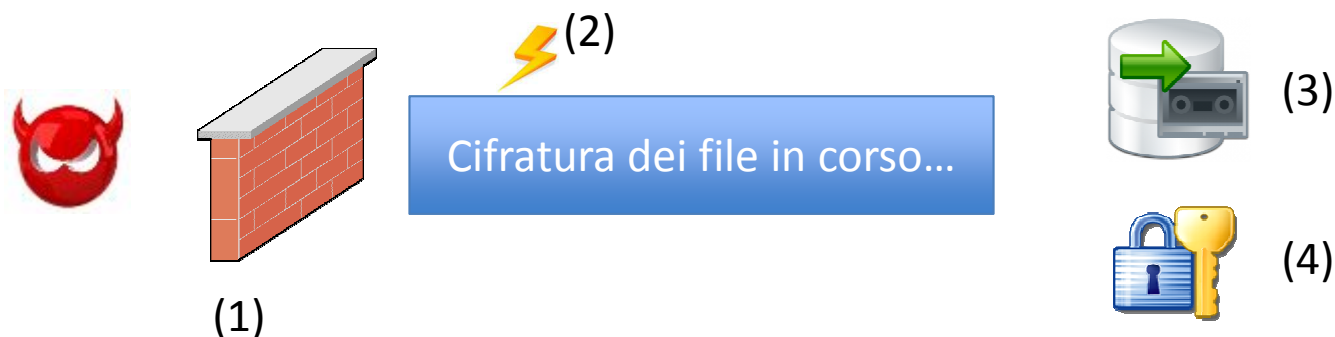
Dist. temporale: num. casi al giorno



## Considerazioni sui CryptoMalware

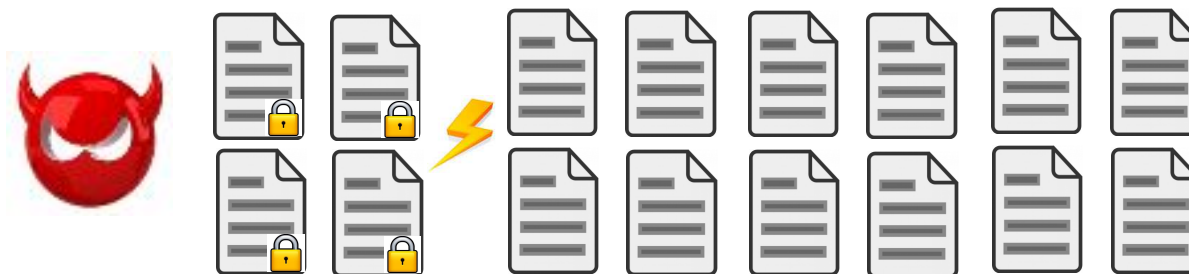
- Il CryptoMalware è una minaccia ATIPICA rispetto a quelle tradizionali (Trojan.Banker, Rootkit, Backdoor, Adware, Virus, etc)
- organizzazioni criminali
- guadagnare soldi (estorsione, richiesta piccola somma)
- non rintracciabili: moneta bitcoin – conti anonimi
- rilascio di nuove varianti di cryptomalware ad ogni ora
- Al cryptomalware è sufficiente essere eseguito solo 1 volta !!!
- Al termine della cifratura si cancella
- Può colpire anche i computer in rete

## Come mi difendo



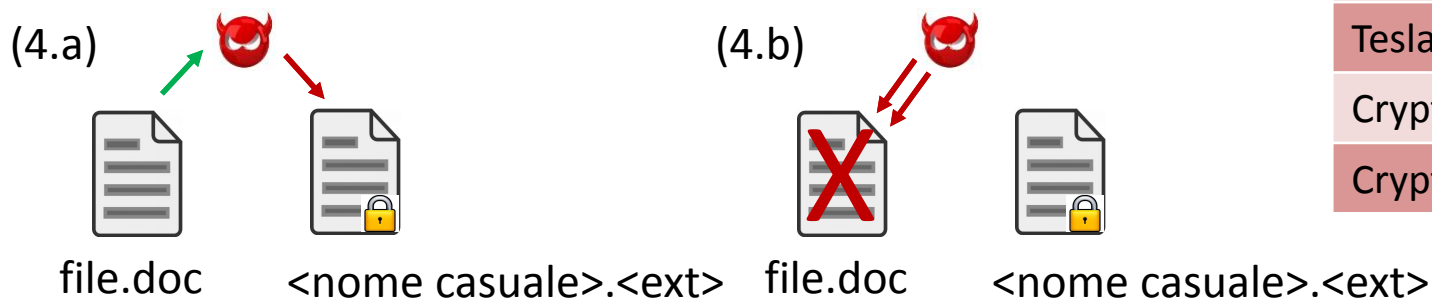
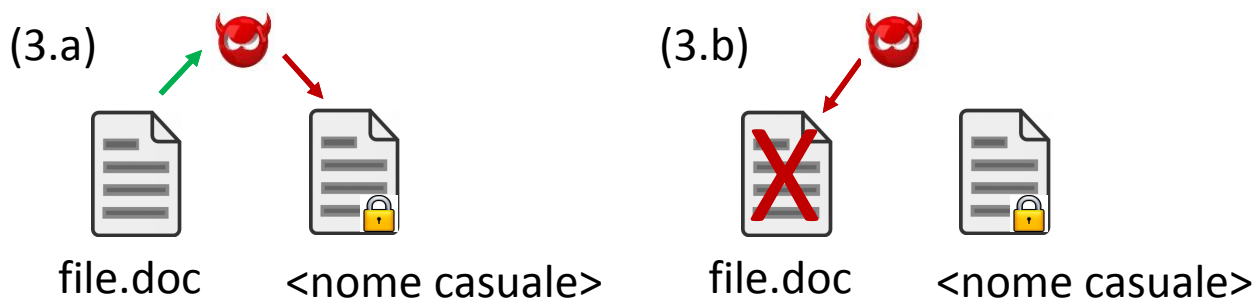
- (1) Bloccare il CryptoMalware prima che arrivi sul PC o che venga eseguito (anti-virus)
- (2) Mitigazione dell'attacco: Protezione Anti-Crypto Malware
- (3) Backup
- (4) Recuperare i file cifrati

## Mitigazione dell'attacco: protezione Anti-Crypto Malware



- E' un approccio euristico, che va ad analizzare il "comportamento" dei processi
- Se il processo si comporta da "cryptomalware", allora la protezione andrà ad inibire l'accesso al file system del processo
- Disattivazione della connessione di rete LAN

# Esempi di schemi di "comportamento" da CryptoMalware



Nome	Tipo
DirtyDecrypt	1
CryptoLocker	2
CTBLocker	2
CryptoEncoder	2
TeslaCrypt	2
CryptoWall 4.0	3
CryptoLocky	4



# VirIT protezione Anti-Crypto Malware

- **Protezione Anti-Crypto Malware:** permette di bloccare cryptomalware anche di nuova generazione
- **Backup on-the-fly:** backup al volo di file documenti (da 2 KB a 3 MB) in fase di cancellazione, vengono tenuti per 48 ore
- **Disattivazione automatica connessione di rete LAN**
- **Protezione da attacco esterno delle cartelle condivise**



# VirIT protezione Anti-Crypto Malware

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)	Si	No	Si
CryptoEncoder	Si	No	-
CryptoFF	Si	No	Si
CryptoWall 4.0	Si	Si	-
CryptoLocky	Si	No	-

## VirIT protezione Anti-Crypto Malware

Simulazione di un attacco da  
CryptoMalware su macchina  
virtuale.

Video su youtube:

[https://youtu.be/\\_SyKqqZu6-8](https://youtu.be/_SyKqqZu6-8)

# VirIT protezione Anti-Crypto Malware

## 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
<b>Efficacia della tecnologia Anti-CryptoMalware integrata in Vir.IT eXplorer PRO</b>	<b>99,63%*</b>

\* Aspettativa percentuale media di file salvati dalla crittografazione grazie alla protezione Anti-CryptoMalware di Vir.IT eXplorer PRO: [http://www.tgsoft.it/italy/news\\_archivio.asp?id=664](http://www.tgsoft.it/italy/news_archivio.asp?id=664)

# Backup

- Il **Backup** è l'unica soluzione che ci permette di recuperare i nostri file
  1. Le copie di "backup" devono essere scollegate dalla rete, per non incorrere nella cifratura da parte del crypto-malware
  2. Tenere più copie di "backup" separate
  3. Non tenere le copie di "backup" sul NAS, pensando che essendo sotto "linux" siano intaccabili !!!
  4. **Dropbox** e la **sincronizzazione**: i file cifrati in locale verranno sincronizzati da Dropbox, in questo modo i file originali verranno sostituiti con quelli cifrati
- **VirIT Backup**: permette di eseguire copie di "backup" come i tradizionali software, ma queste saranno protette contro la cifratura

## Punti di criticità dei sistemi di Backup:

- Tempo per eseguire il backup o il ripristino dei dati
- Copie obsolete



## E' possibile recuperare i file cifrati ?

- L'utilizzo di algoritmi di cifratura come **AES o RSA**, rende il recupero dei file cifrati nella maggior parte dei casi di difficile realizzazione, a meno che non si conosca la chiave utilizzata
- In passato sono state recuperate le **chiavi private dal server di C/C**, grazie all'ausilio delle forze dell'ordine (sequestro del computer)
- In alcuni casi gli autori dei crypto-malware hanno commesso degli errori e hanno lasciato dei punti deboli nel loro sistema, come nel caso del **TeslaCrypt** (versioni precedenti alla 3.0)
- In altri è possibile recuperare i file cifrati attraverso le **shadow copies** di Windows (da Vista in su), se queste non sono state cancellate dal crypto-malware.
- Con software di recupero dati (come Recuva) è possibile ripristinare file "accidentalmente" cancellati

# TeslaCrypt

Per le versioni precedenti alla 3.0 del TeslaCrypt (.vvv e altre) è possibile recuperare i file con i seguenti 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**

Il **teorema fondamentale dell'aritmetica** afferma che:

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.

$$n = p_1 * p_2 * \dots * p_k$$

Attraverso la fattorizzazione è stato possibile determinare la chiave privata.

# TeslaCrypt 3.0

- Dalla versione 3.0 del TeslaCrypt (.micro e .mp3) **NON è possibile recuperare i file** (senza conoscere la chiave privata), perchè gli autori hanno corretto l'errore introdotto nelle versioni precedenti.
- La chiave privata è un numero casuale a 256 bit
- La chiave pubblica è un punto della curva ellittica secp256k1

## Numero di combinazioni:

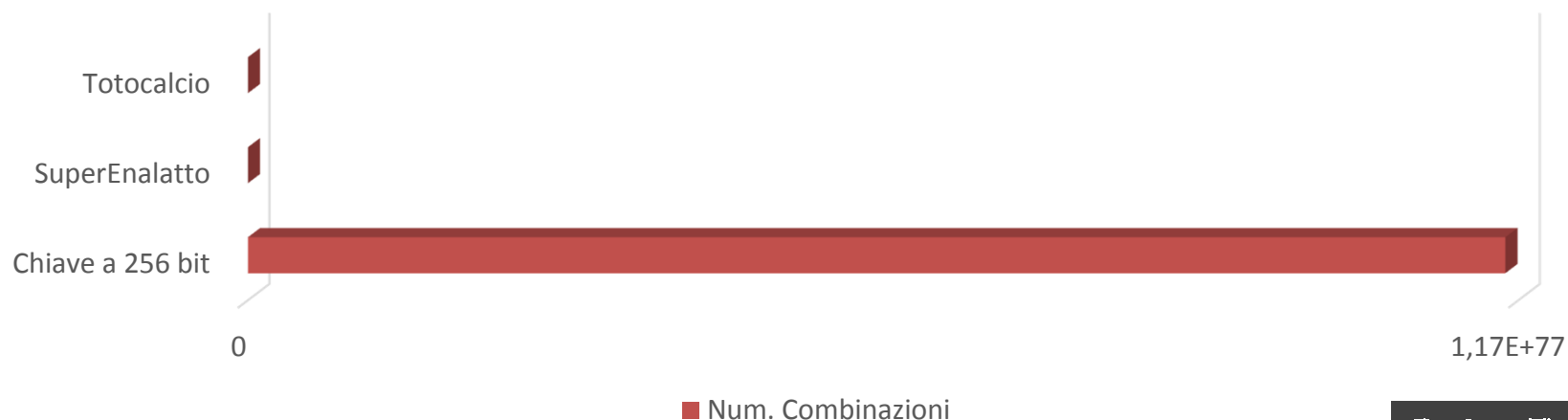
Totocalcio (13 partite) =  $3^{13} = 1594323$

SuperEnalotto =  $C(90,6) = 622614630$

Chiave a 256 bit =

115792089237316195423570985008687907853269984665640564039457584007913129639935

Nel 2004 per risolvere una curva ellittica a 109 bit, un team di 2600 persone ha impiegato 17 mesi.



## Conclusioni

- Nei primi 2 mesi del 2016 abbiamo visto un'impennata di crypto-malware rispetto al 2015
- Gli autori sono vere e proprie organizzazioni criminali, che lavorano a livello industriale, sfornando ad ogni ora nuove varianti di Crypto-Malware
- I classici prodotti AV sono in difficoltà contro queste tipologie di minacce
- Il recupero dei file cifrati è molto difficile, a meno che non vi siano errori da parte degli autori dei crypto-malware
- Il riscatto richiesto è una somma "bassa", pagare o non pagare ?
- Il backup è un'ottima soluzione, ma non sempre viene eseguito oppure quando non viene cifrato può essere obsoleto
- La protezione pro-attiva Anti-Crypto malware può mitigare l'attacco salvando la vittima

# Domande





**smau** 

**PADOVA** 10-11 MARZO 2016

**Autore**

Ing. Gianfranco Tonello ([g.tonello@viritpro.com](mailto:g.tonello@viritpro.com))

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

Grazie per l'attenzione

**TG Soft**  
Software House  
[www.tgsoft.it](http://www.tgsoft.it)



<https://www.facebook.com/viritexplorer>



PadovaFiereSpa

## Referenze

- <http://www.tgsoft.it>
- [https://www.youtube.com/watch?v=\\_SyKqqZu6-8&feature=youtu.be](https://www.youtube.com/watch?v=_SyKqqZu6-8&feature=youtu.be)
- TeslaDecoder: <http://www.bleepingcomputer.com/forums/t/576600/tesldecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/>
- TeslaCrack: <https://github.com/Googulator/TeslaCrack>
- The Talos TeslaCrypt Decryption Tool: <http://blogs.cisco.com/security/talos/teslacrypt>
- Let's ride with TeslaCrypt: <http://thisissecurity.net/2016/03/02/lerts-ride-with-teslacrypt/>