smau

PADOVA 10-11 MARZO 2016

Scacco matto ai Crypto-Malware!

Come mettere al sicuro i nostri dati più preziosi.

PadovaFiereSpa

Ing. Gianfranco Tonello

smau

PADOVA 10-11 MARZO 2016

Scacco matto ai Crypto-malware!

PadovaFiereSpa

Ransomware: cosa sono ?

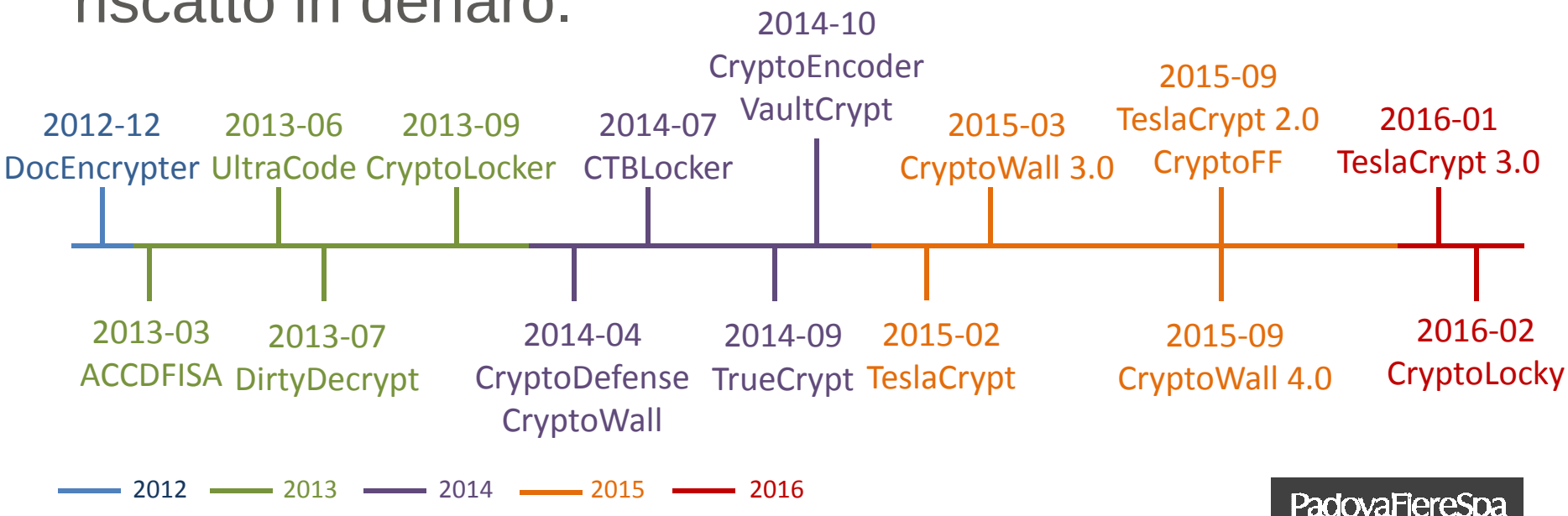
Con il termine **Ransomware** definiamo tutti quei programmi o software che bloccano l'accesso ai file di documenti o al computer chiedendo un riscatto in denaro per accedervi.

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**


Da: Enel Spa <mcsrl@sicurezzapostale.it>
A: Carrozzeria Baggio
Cc:
Oggetto: Carrozzeria Baggio bolletta per la fornitura di energia elettrica

Enel
L'ENERGIA CHE TI ASCOLTA
Enel ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE

Numero cliente: 59 369 524 Codice Fiscale: EPDZH02565QI

Carrozzeria Baggio

BOLLETTA PER LA FORNITURA DI ENERGIA ELETTRICA
N. fattura 499933859 del 1/03/2016 Bimestre gennaio - febbraio 2016
Totale da pagare entro il 31/03/2016: euro 336,10

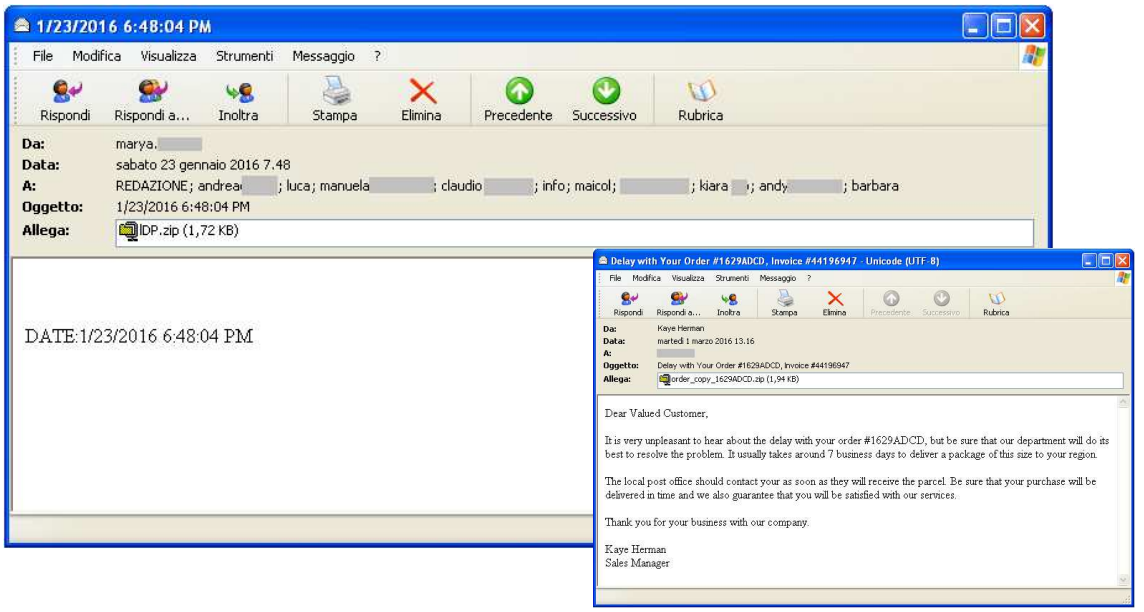
Come da lei richiesto, sar` addebitato nel giorno esatto della scadenza su conto corrente presso: 5330119521
Clicca qui per scaricare

DATI FORNITURARIEPILOGO IMPORTI FATTURATIL

Politica sulla privacy

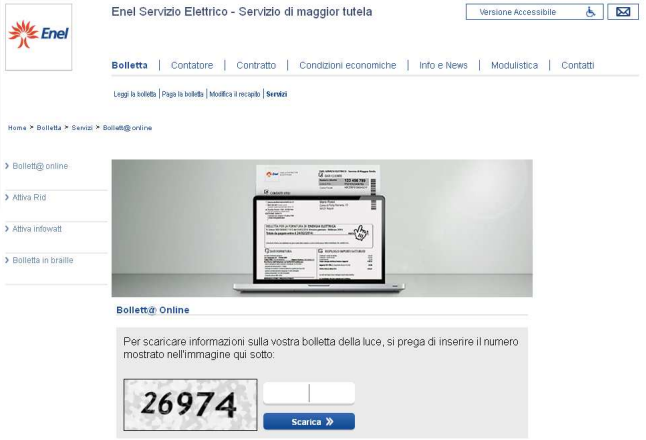
Enel adotta un apposito regolamento per la gestione ed il trattamento delle informazioni riservate, contenente anche le procedure per la comunicazione all'esterno di documenti ed informazioni concernenti Enel, con particolare riferimento alle informazioni privilegiate. Gli esponenti aziendali, i dipendenti e i collaboratori di Enel evitano comportamenti che possano dare luogo a fenomeni di insider trading e di manipolazione del mercato, anche da parte di terzi; al fine di garantire la massima trasparenza risultano adottate al riguardo procedure in materia di internal dealing rispettose della legge ed in linea con le best practice internazionali. Nel bilancio annuale sono pubblicate le azioni Enel possedute al termine dell'esercizio, nonch'e gli acquisti e le vendite effettuate nel corso dell'esercizio stesso, da parte dei membri del consiglio di amministrazione, dei sindaci e dei dirigenti con responsabilit`a strategiche di Enel S.p.A.. Enel ha istituito (e tiene regolarmente aggiornato) un registro in cui risultano iscritte le persone, fisiche o giuridiche, che hanno accesso ad informazioni privilegiate in ragione dell'attivit`a lavorativa o professionale ovvero delle funzioni svolte per conto di Enel. Tale registro ha la finalit`a di sensibilizzare i soggetti ivi iscritti sul valore delle informazioni privilegiate di cui dispongono, agevolando al contempo lo svolgimento delle attivit`a di controllo da parte dell'Autorit`a di vigilanza sul rispetto delle norme previste a tutela dell'integrit`a dei mercati.

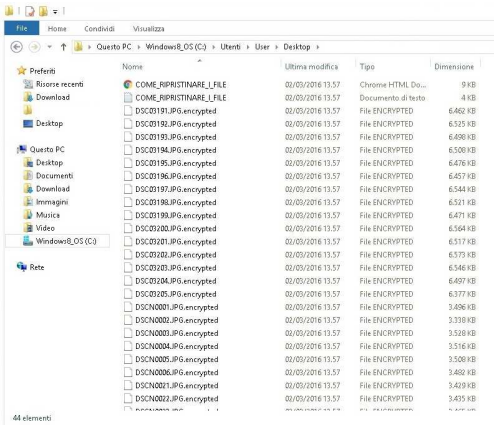
clicca qui per cancellare l'iscrizione (unsubscribe)

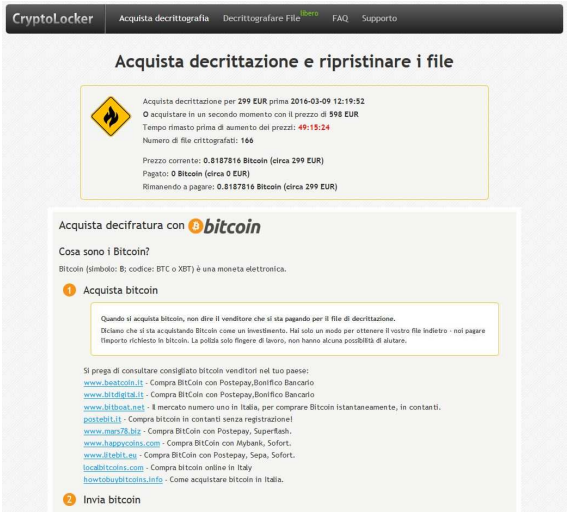


CryptoLocker - TorrentLocker

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

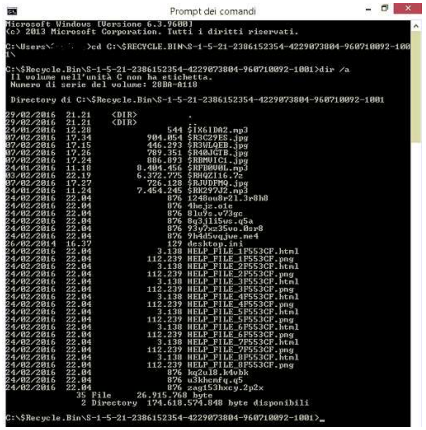






CryptoWall

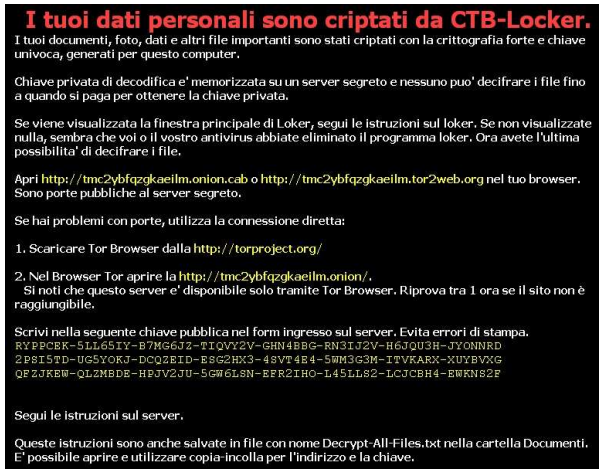
- anno: 2014 aprile
- estensione: <casuale>
- algoritmo: RSA-2048
- riscatto: 500/1000 USD (in bitcoin)
- rete: Tor-Onion
- versione: 4.0

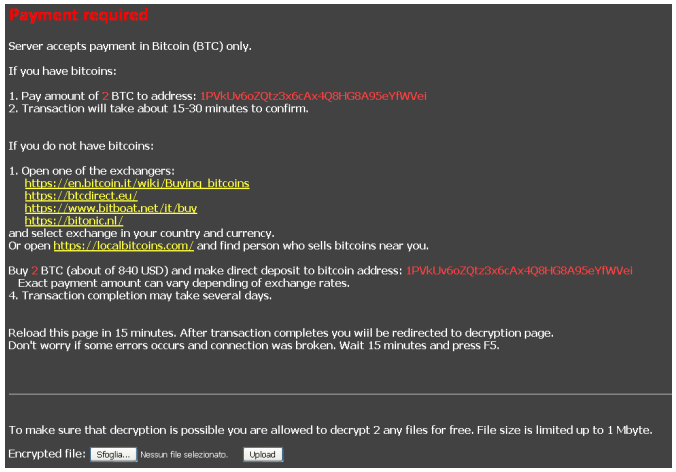


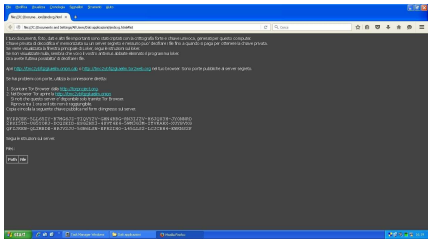
PadovaFiereSpa

CTBLocker: Curve Tor Bitcoin Locker

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

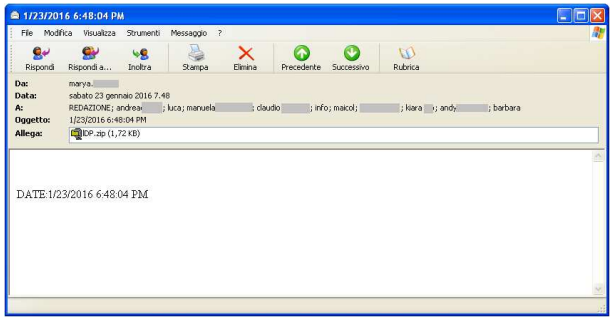


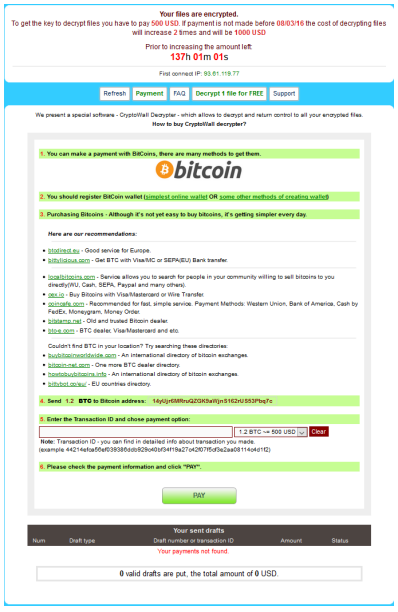


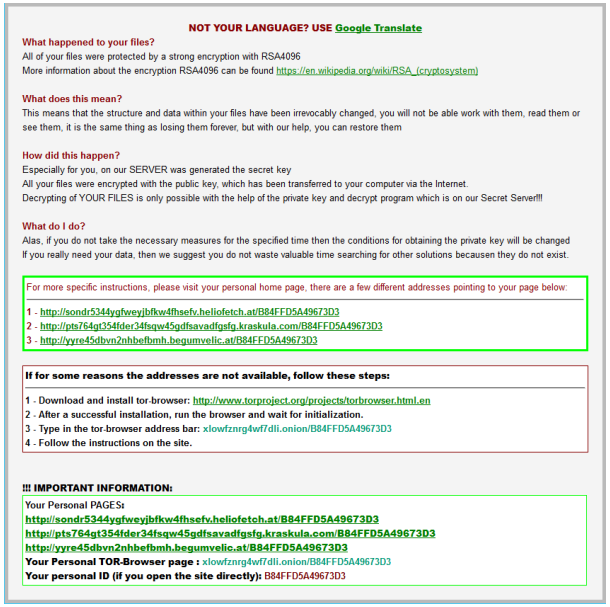


TeslaCrypt

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







CryptoLocky

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

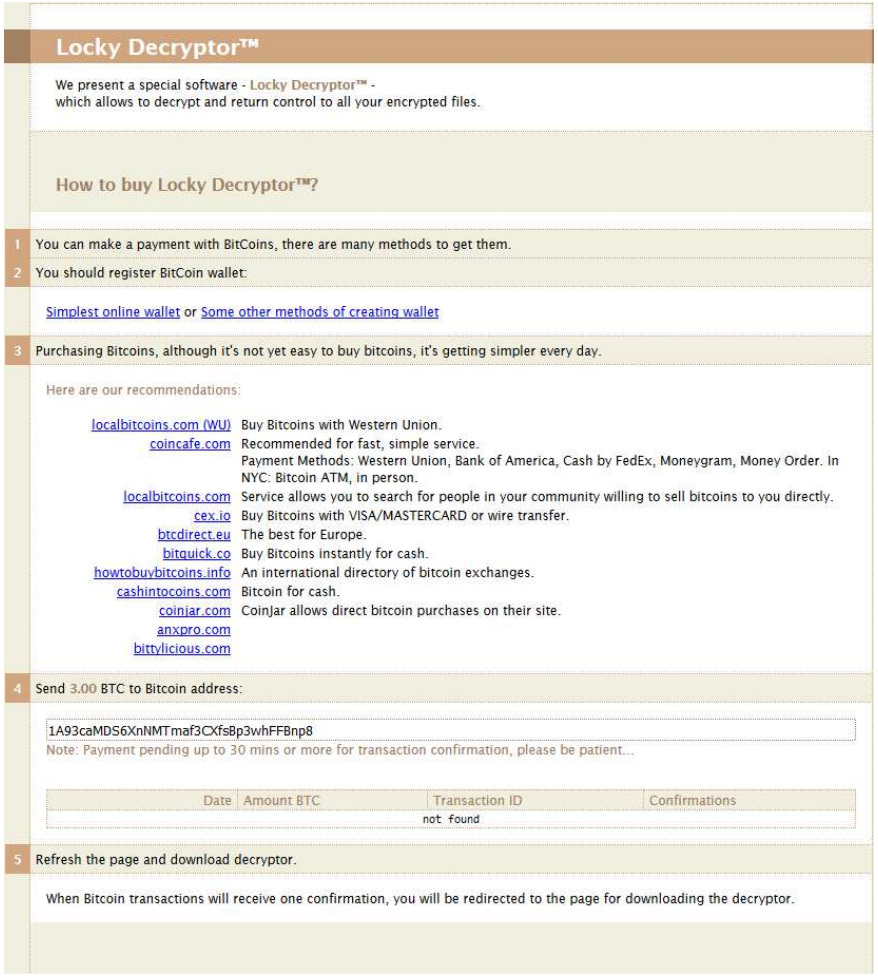
!!! INFORMAZIONI IMPORTANTI!!!!

Tutti i tuoi file sono stati criptati con algoritmo asimettrico 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
4. Segui le istruzioni a video.

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



Come funziona il CryptoMalware

email o sito infetto

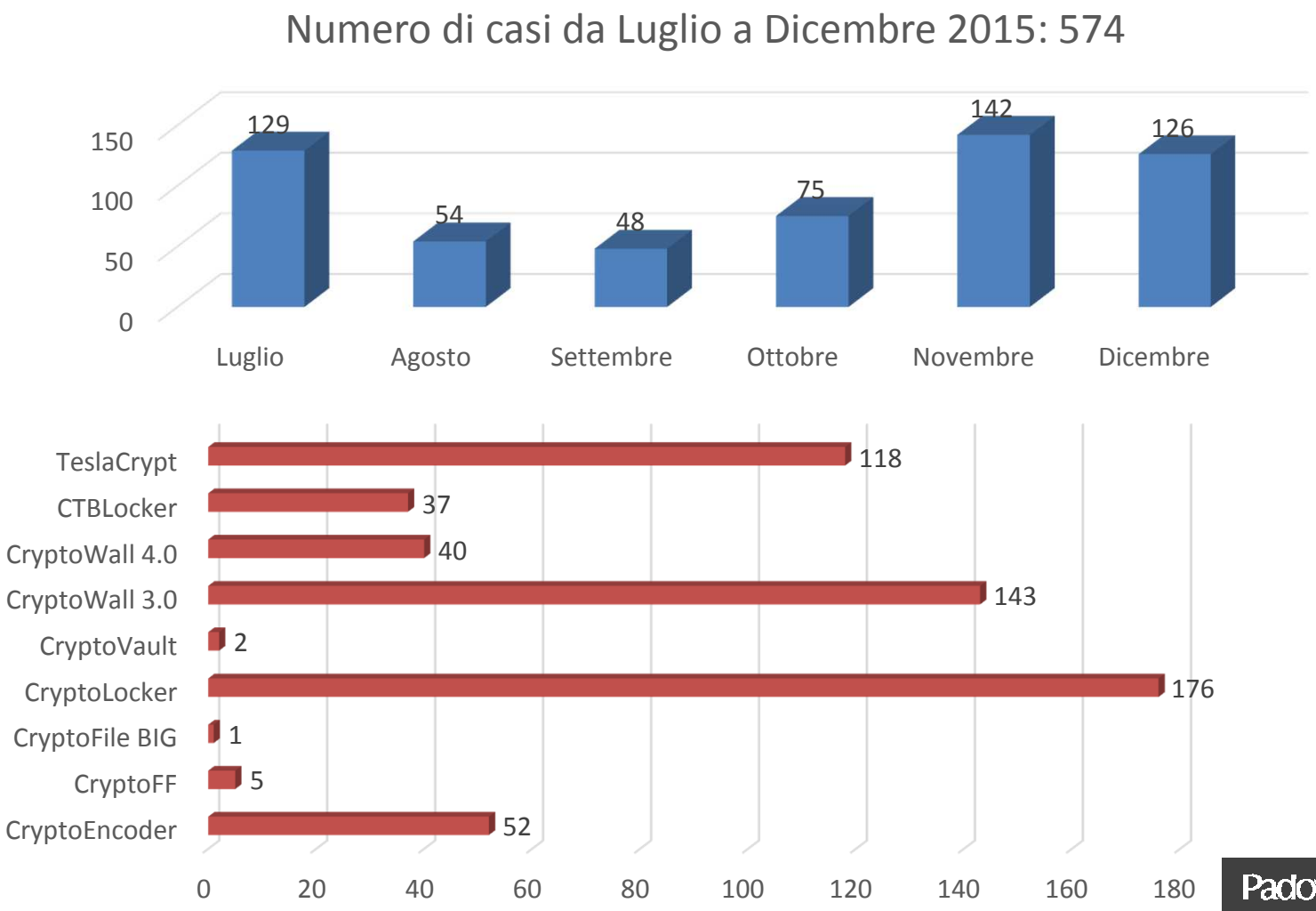
esecuzione cryptomalware

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

cifratura documenti locali e di rete

richiesta riscatto

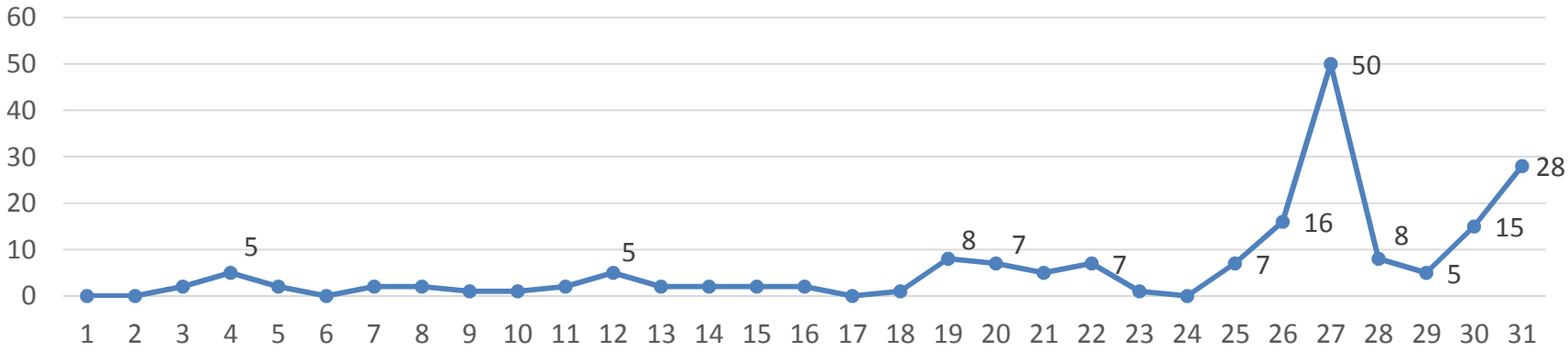
Statistiche: da Luglio a Dicembre 2015 (Italy)

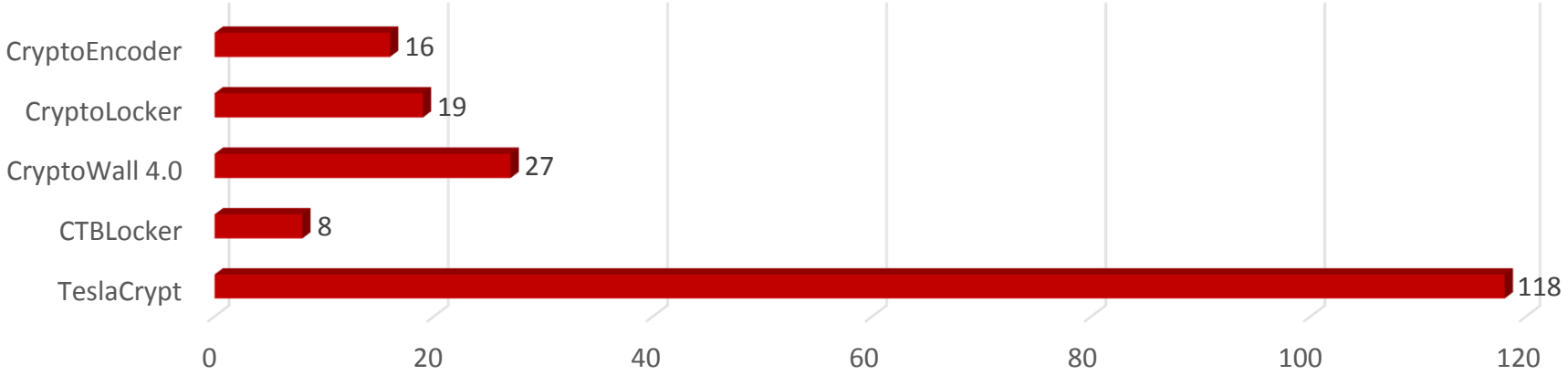


Statistiche: Gennaio 2016 (Italy)

Num. casi: 188

Dist. temporale: num. casi al giorno

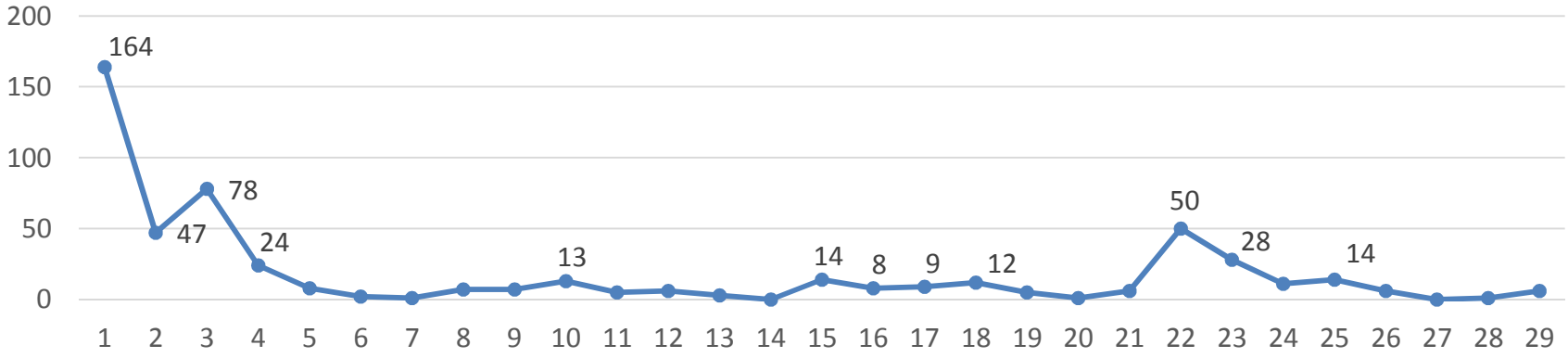


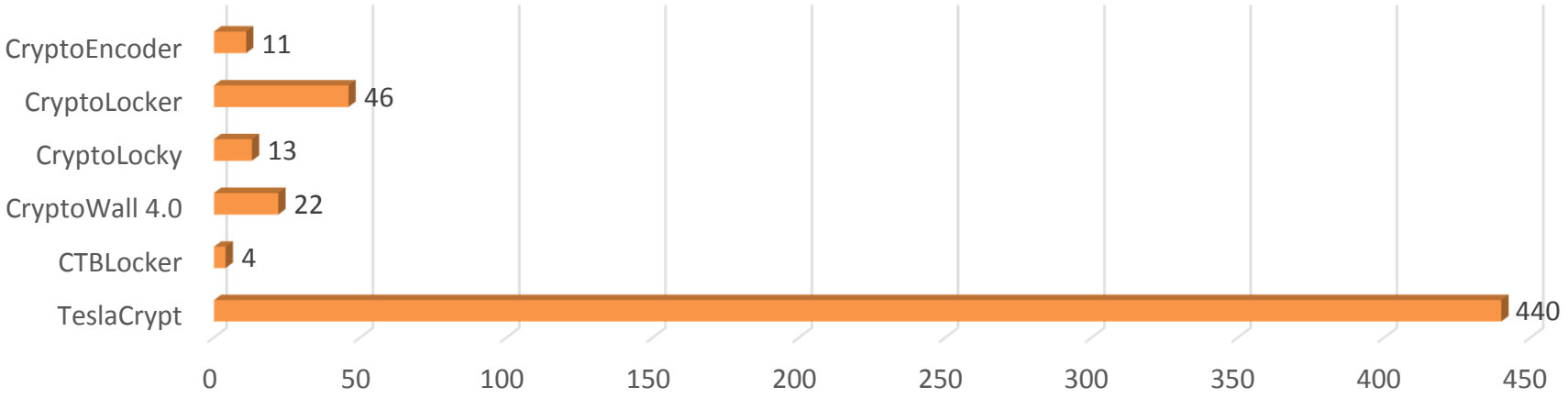


Statistiche: Febbraio 2016 (Italy)

Num. casi: 536

Dist. temporale: num. casi al giorno

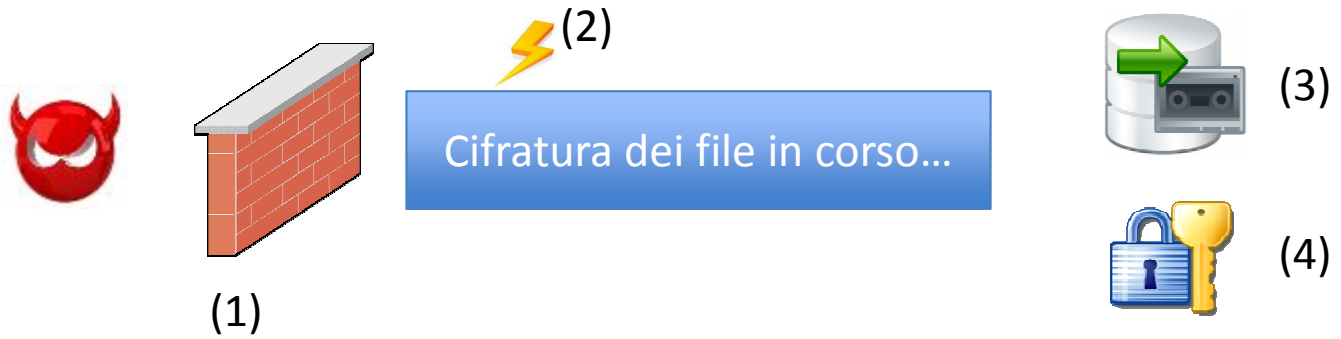




Considerazioni sui CryptoMalware

- 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

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
Efficacia della tecnologia Anti-CryptoMalware integrata in Vir.IT eXplorer PRO	**99,63%***

* Aspettativa percentuale media di file salvati dalla crittografazione grazie alla protezione Anti-CryptoMalware di Vir.IT eXplore PRO: 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 verrano sincronizzati da Dropbox, in questo modo i file originali verranno sostituti 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 algortimi 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 precendenti 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 precendenti 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.

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

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

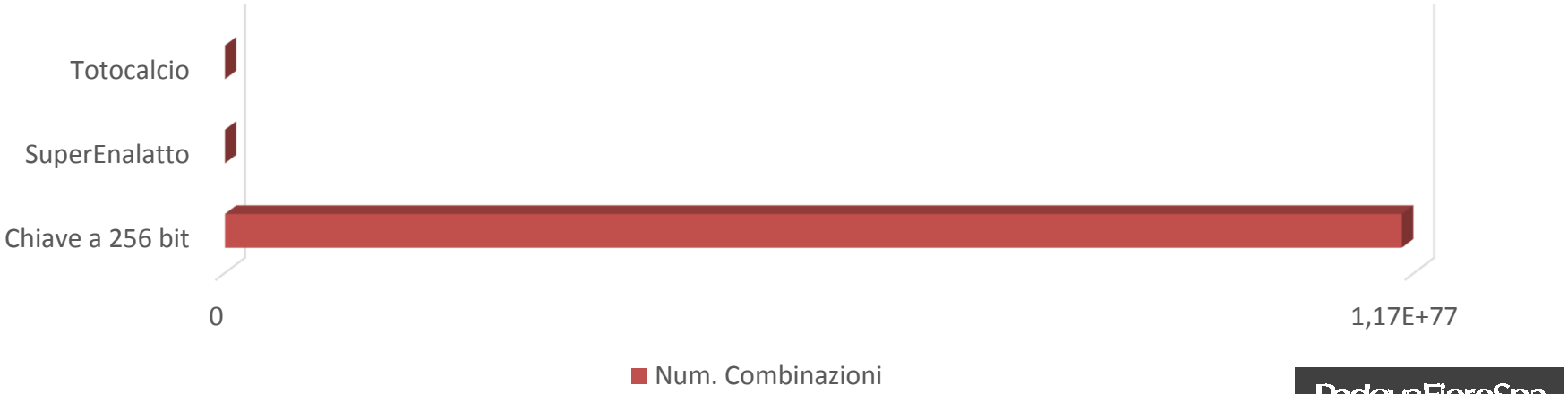
Nel 2004 per risolvere una curva ellittica a 109 bit, un team di 2600 persone ha impiegato 17 mesi.

Numero di combinazioni:

Totocalcio (13 partite) = 3^13 = 1594323

SuperEnalotto = C(90,6) = 622614630

Chiave a 256 bit = 115792089237316195423570985008687907853269984665640564039457584007913129639935



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

Autore

Ing. Gianfranco Tonello (g.tonello@viritpro.com)
https://it.linkedin.com/in/gianfranco-tonello-77078843

Grazie per l'attenzione

TG Soft
Software House
www.tgsoft.it

https://www.facebook.com/viritexplorer

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

Referenze

- http://www.tgsoft.it
- https://www.youtube.com/watch?v=_SyKqqZu6-8&feature=youtu.be
- TeslaDecoder: http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-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/lets-ride-with-teslacrypt/