Κλεισμένοι έξω από τα δεδομένα μας

Παναγιώτης Πιέρρος
Managing Director
TicTac Data Recovery

Μιχάλης Μίγγος
Technical Director
TicTac Data Recovery

Case Studies από το εργαστήριο της TicTac Data Recovery.
Πως αντιμετωπίσαμε την απώλεια, τη διαρροή και την κρυπτογράφηση και οι λύσεις που προτείνουμε το 2016

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Όταν δεν έχετε πρόσβαση στα δεδομένα σας… τότε αναλαμβάνει δράση η TicTac Laboratories

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Τι θα δούμε στα επόμενα 13 λεπτά

1. **Γιατί αφού όλοι γνωρίζουν το backup στην TicTac έχουμε ακόμα δουλειά;**
2. **Περιπτώσεις Ransomware (Locky, Cryptowall & TeslaCrypt):** Το χρονικό της ζημιάς και τα στατιστικά επιβίωσης από μια επίθεση
3. Η αποτελεσματικότερη προστασία – Disaster Recovery by StorageCraft RecoverAbility
4. DRP : Data Rescue Plan
5. Υπηρεσίες που προσφέρουν λύσεις σε προβλήματα
6. 11 πρακτικές συμβουλές για να μην έχουμε επισκέψεις από τον Cryptowall και το… συνάφι του

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Ξέρετε αλήθεια τι είναι το backup?

Η διατήρηση των κρίσιμων δεδομένων μας σε δύο τουλάχιστον αντίγραφα (και ιδανικά από διαφορετικές χρονικές στιγμές) τα οποία βρίσκονται σε ανεξάρτητο μέσο και σε ανεξάρτητο φυσικό χώρο

- **Ανεξάρτητο Φυσικό μέσον** από το βασικό μέσον αποθήκευσης
- **2 ταυτόχρονα αντίγραφα τουλάχιστον σε διαφορετικό μέσον και φυσικό χώρο**
- **Θα πρέπει να υπάρχουν διαφορετικές εκδόσεις των αρχείων μας**

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

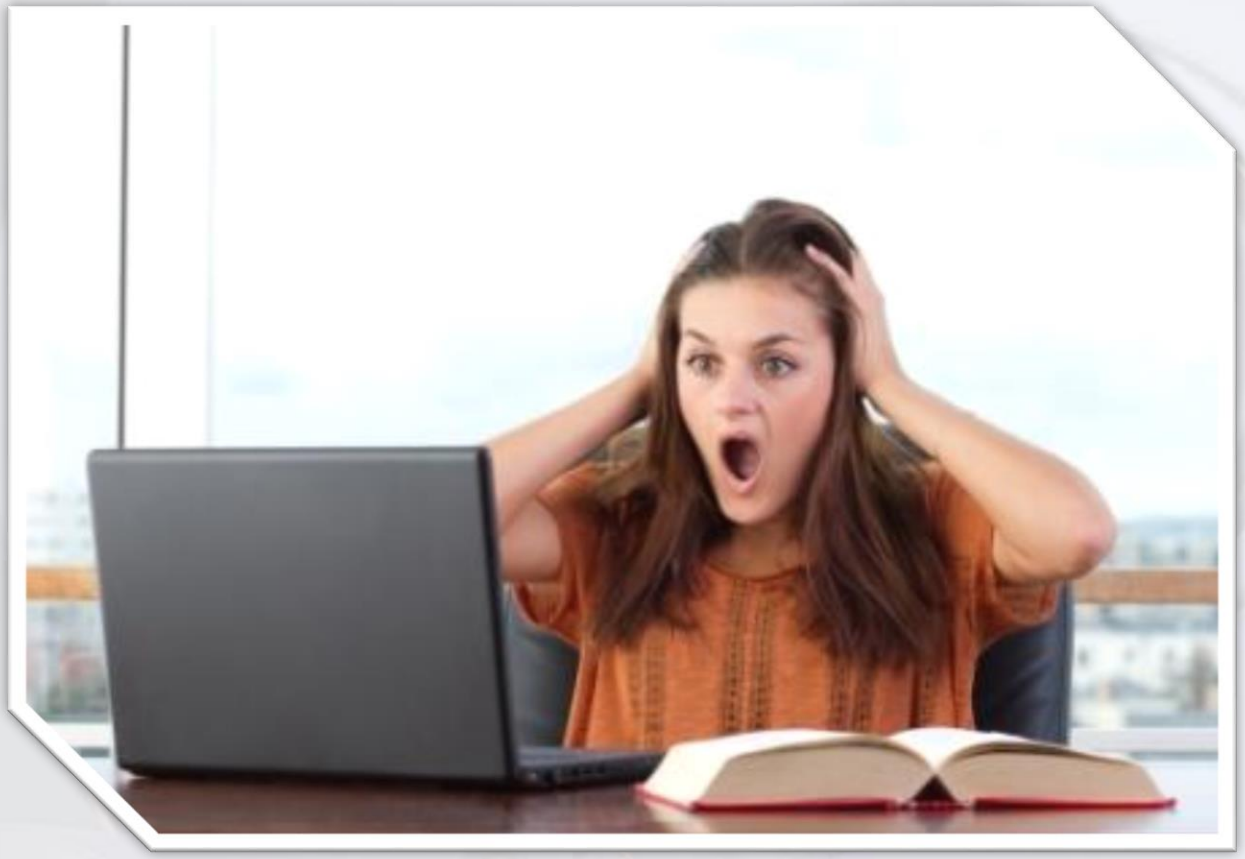
Τι δεν είναι Backup

1. Αντιγράφω τον C:\ στον D:\ (ενώ βρίσκονται στον ίδιο σκληρό δίσκο τα partitions)
2. Κάνω Backup τις φωτογραφίες μου στον εξωτερικό δίσκο για να απελευθερώσω χώρο από το Laptop μου.
3. Βάζω τα αρχεία Word και Excel στο Cloud, άρα κάνω backup σωστό!
4. Έχω ένα NAS με Raid 0

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Έχεις κάνει backup το κινητό σου;

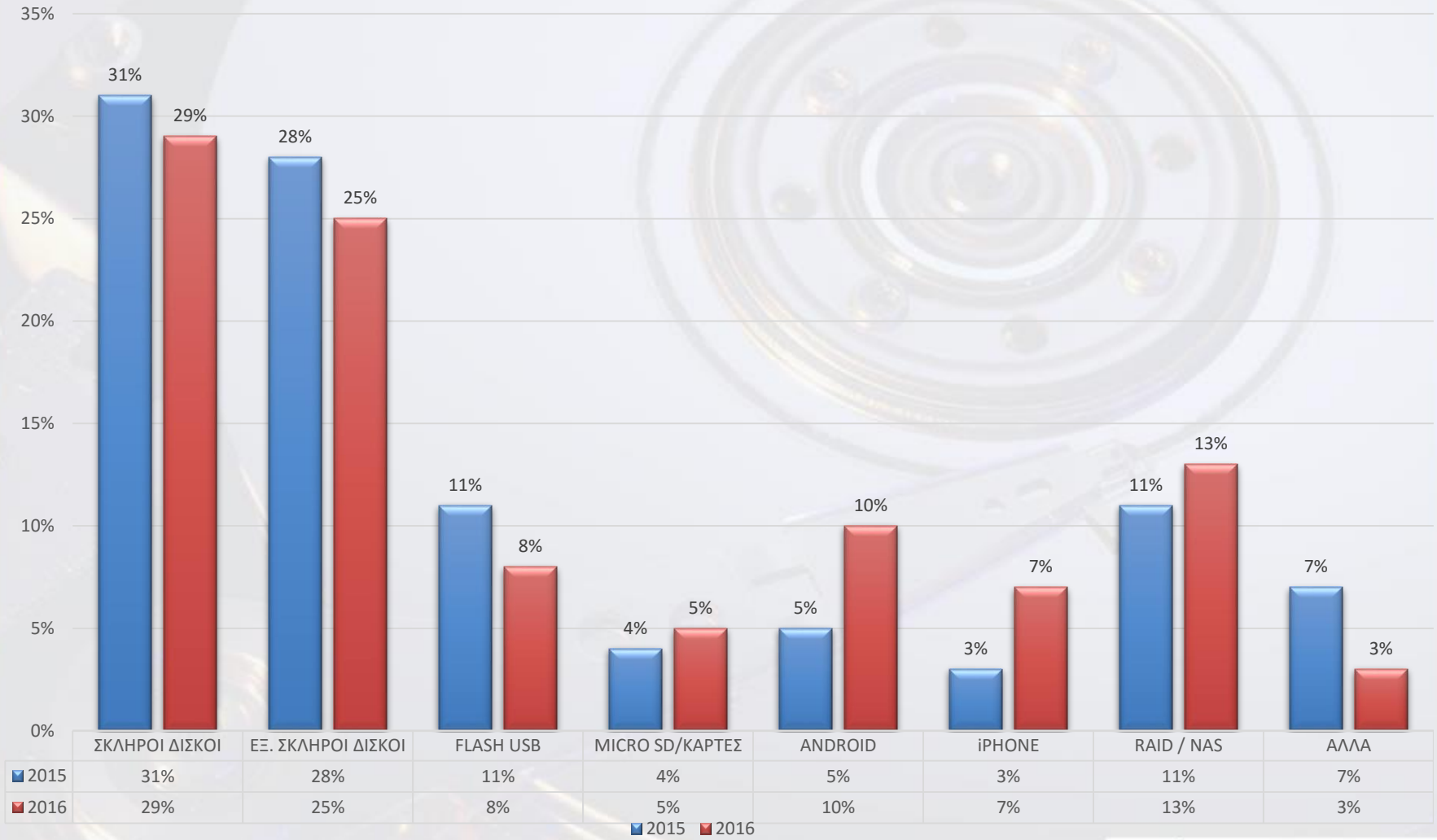
TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr



Υποθέσεις Data Recovery

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

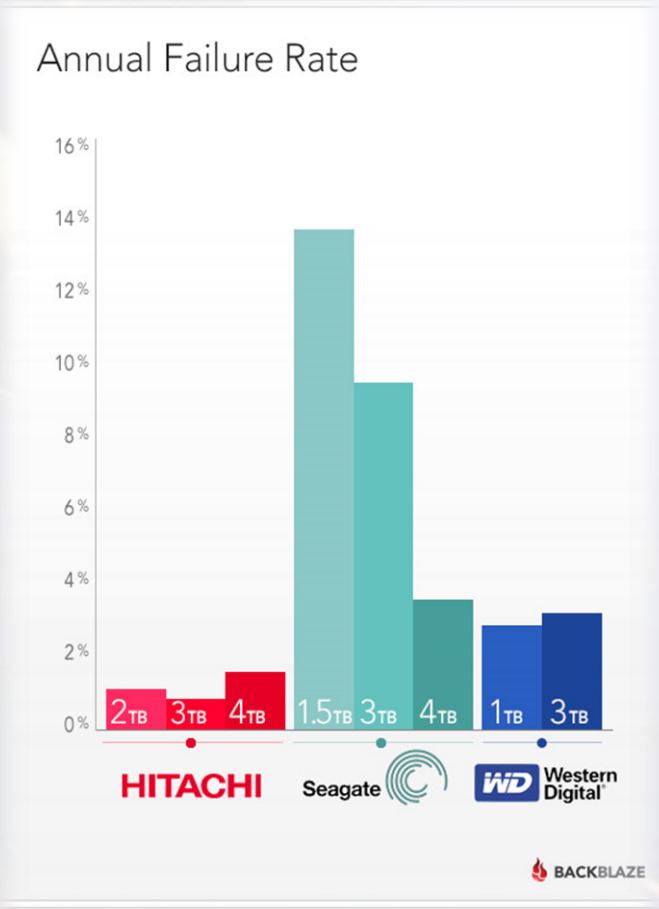
Ποσοστά Υποθέσεων ανά είδος μέσου 2015 - 2016



	ΣΚΛΗΡΟΙ ΔΙΣΚΟΙ	ΕΞ. ΣΚΛΗΡΟΙ ΔΙΣΚΟΙ	FLASH USB	MICRO SD/ΚΑΡΤΕΣ	ANDROID	iPHONE	RAID / NAS	ΑΛΛΑ
2015	31%	28%	11%	4%	5%	3%	11%	7%
2016	29%	25%	8%	5%	10%	7%	13%	3%

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Στατιστικά από το εργαστήριο & συμπεράσματα



1. **5-10% των δίσκων παρουσιάζουν αστοχία υλικού στην 3ετία**
2. Είδαμε δίσκους **3TB-4TB να χαλάνε 20-30 ημέρες** από την αγορά τους
3. Πολλοί **SSD δίσκοι συνάντησαν με ελαττωματικό firmware**
4. Εκατοντάδες **επώνυμα USB Flash Disks σταμάτησαν να λειτουργούν ξαφνικά**
5. Σε **συστοιχίες Raid «χτύπησαν» ταυτόχρονα πολλαπλοί δίσκοι**
6. Όσο μεγαλώνουν οι χωρητικότητες **αυξάνονται τα προβλήματα** και ο **όγκος των δεδομένων που χάνεται**
7. **9%** των υποθέσεων ήταν **μη ανακτήσιμες** όταν παραλάβαμε **λόγω επέμβασης (2015), 3% αύξηση από το 2014**

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Ατυχή περιστατικά απώλειας

1. Σε **πολύ μεγάλο δημόσιο οργανισμό υγείας** ένα σύστημα Raid 5 – 15 δίσκων και συνολικής χωρητικότητας 12TB, το οποίο γινόταν Replicate σε αντίστοιχο Raid σύστημα μετά από προβλήματα στην ηλεκτροδότηση επήλθε απώλεια δεδομένων. **Έχασε ιστορικό ασθενών 10ετίας**. Ανακτήθηκε μετά από εντατική προσπάθεια 2 μηνών.
2. Σε κατασκευαστική εταιρία έτυχαν **18 περιστατικά χαλασμένων δίσκων** εντός του ίδιου έτους σε διαφορετικές χρονικές στιγμές.
3. Σε **μεγάλη επιχείρηση** , την ώρα που ο τεχνικός έπαιρνε backup σε εξωτερικό δίσκο, έπεσε το ρεύμα και χάθηκαν και οι δύο δίσκοι
4. **Δικηγορικό γραφείο** διατηρούσε backup 15ετίας σε usb flash 512mb το οποίο χάλασε και δεν υπηρχε Backup.

Λύση: Backup σε 2-3 σημεία ακόμα και offsite, με versioning.

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Στην μόδα φέτος ο «Locky”
και ο TeslaCrypt

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Ο Locky εν δράσει…

Sen_Installation_Files	16/3/2016 5:26 μμ	File folder	
Tax-Free	30/4/2010 7:12 μμ	File folder	
WINDOWS	16/3/2011 3:35 μμ	File folder	
WindowsImageBackup	1/7/2013 5:56 μμ	File folder	
wmpub	7/1/2010 4:26 μμ	File folder	
_Locky_recover_instructions	16/3/2016 5:23 μμ	Text Document	2 KB
976B7147270D792C3CE707E70832A86D.locky	16/3/2016 5:24 μμ	LOCKY File	5 KB
976B7147270D792C7FC9EE5648F41F24.locky	16/3/2016 5:26 μμ	LOCKY File	14.451 KB
976B7147270D792C29BB7986DB8C8190.locky	16/3/2016 5:26 μμ	LOCKY File	115.350 KB
976B7147270D792C33C4ABDA090A9BE5.locky	16/3/2016 5:26 μμ	LOCKY File	58.451 KB

Organize ▾ Include in library ▾ Share with ▾ Burn New folder

Pictures
Videos
Computer
Local Disk (C:)
Local Disk (E:)
New Volume (F:)
Seagate Backup Plu
KINGSTON (H:)
KARPODINIS softw

Name	Date modified	Type	Size
E	7/10/2013 8:39 μμ	File folder	
ΕΝΤΥΠΑ ΕΦΟΡΙΑΣ	28/4/2014 9:04 πμ	File folder	
_Locky_recover_instructions	16/3/2016 5:39 μμ	Text Document	2 KB
976B7147270D792C10AA8EDB69059796.locky	16/3/2016 5:39 μμ	LOCKY File	80 KB
ΒΕΒΑΙΩΣΗ ΑΜΚΑ	1/7/2013 11:13 μμ	Adobe Acrobat Doc...	56 KB
Ο.Α.Ε.Ε.	1/7/2013 11:13 μμ	Adobe Acrobat Doc...	79 KB
ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΕΠΟΙΜΕΛΗΤΗΡΙΟ ΚΑΣΤΟΡΙΑΣ	1/7/2013 11:13 μμ	Adobe Acrobat Doc...	62 KB

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Το ραβασάκι…

_Locky_recover_instructions - Notepad

File Edit Format View Help

```
            !!! 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 ou
To receive your private key follow one of the links:
    1. http://i3ezlvkoi7fwyood.tor2web.org/976B7147270D792C
    2. http://i3ezlvkoi7fwyood.onion.to/976B7147270D792C
    3. http://i3ezlvkoi7fwyood.onion.cab/976B7147270D792C

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: i3ezlvkoi7fwyood.onion/976B7147270D792C
    4. Follow the instructions on the site.

!!! Your personal identification ID: 976B7147270D792C !!!
```

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Δεχόμαστε και κάρτες...

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 2.00 BTC to Bitcoin address:

1Hc1FKxayqVJKZxABUKAMXEFh1be59uaQ9

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

Date	Amount BTC	Transaction ID	Confirmations
not found			

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

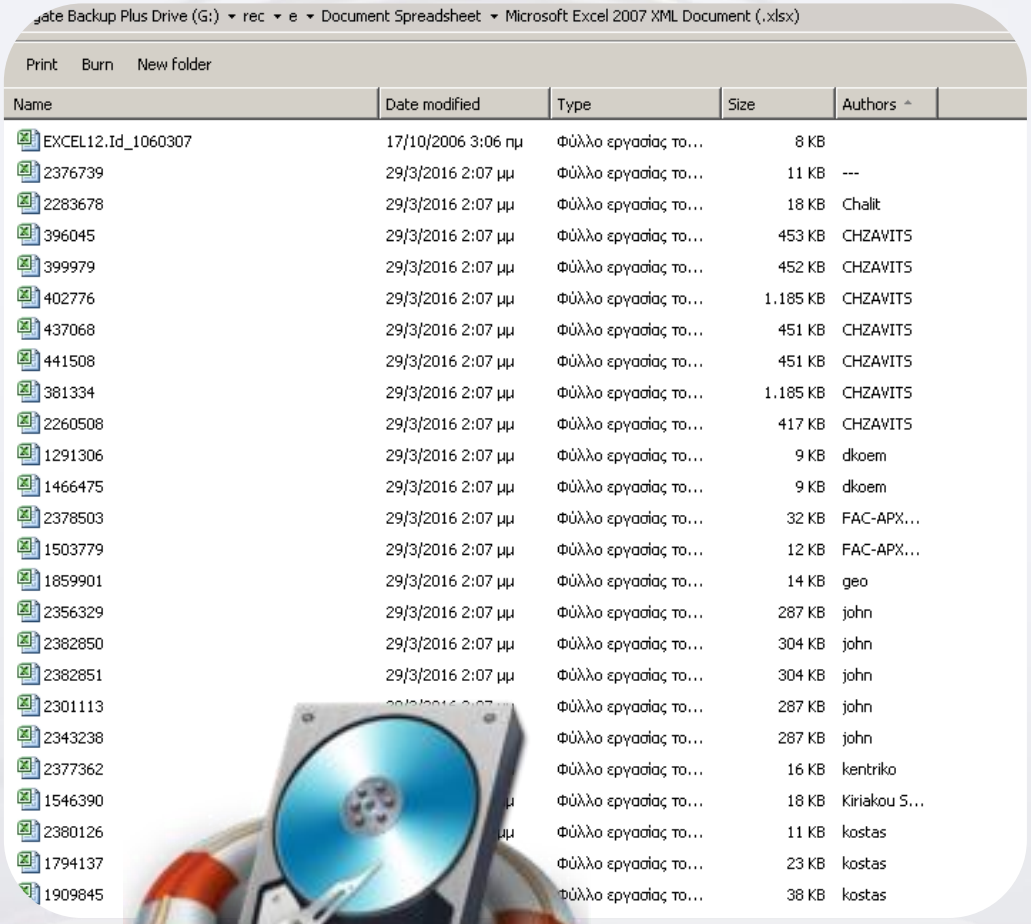
Υπάρχει ελπίδα;

Locky

30% ανακτήσιμα αρχεία

TeslaCrypt

80% + ανακτήσιμος



Name	Date modified	Type	Size	Authors
EXCEL12.Id_1060307	17/10/2006 3:06 πμ	Φύλλο εργασίας το...	8 KB	
2376739	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	11 KB	---
2283678	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	18 KB	Chalit
396045	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	453 KB	CHZAVITS
399979	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	452 KB	CHZAVITS
402776	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	1.185 KB	CHZAVITS
437068	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	451 KB	CHZAVITS
441508	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	451 KB	CHZAVITS
381334	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	1.185 KB	CHZAVITS
2260508	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	417 KB	CHZAVITS
1291306	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	9 KB	dkoem
1466475	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	9 KB	dkoem
2378503	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	32 KB	FAC-APX...
1503779	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	12 KB	FAC-APX...
1859901	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	14 KB	geo
2356329	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	287 KB	john
2382850	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	304 KB	john
2382851	29/3/2016 2:07 μμ	Φύλλο εργασίας το...	304 KB	john
2301113	[illegible]	Φύλλο εργασίας το...	287 KB	john
2343238	[illegible]	Φύλλο εργασίας το...	287 KB	john
2377362	[illegible]	Φύλλο εργασίας το...	16 KB	kentriko
1546390	[illegible]	Φύλλο εργασίας το...	18 KB	Kiriakou S...
2380126	[illegible]	Φύλλο εργασίας το...	11 KB	kostas
1794137	[illegible]	Φύλλο εργασίας το...	23 KB	kostas
1909845	[illegible]	Φύλλο εργασίας το...	38 KB	kostas

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Οι απειλές είναι πολλές

Ποιος μπορεί να δώσει μια απλή λύση για όλα;

Καθημερινά αντιμετωπίζουμε περιστατικά με πελάτες χωρίς backup ή με restore που απέτυχε!

Η προτεινόμενη ολοκληρωμένη λύση…
StorageCraft RECOVER-Ability

Υβριδικό & αυτοματοποιημένο Disaster Recovery τοπικά και στο Cloud με versioning

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

STORAGECRAFT.

RECOVER-ABILITY™ SOLUTION

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

DRP by GENERALI

Data Rescue Plan

Για πρώτη φορά στην Ελλάδα μια μεγάλη καινοτομία στο χώρο της τεχνολογικής ασφάλισης

Δίνεται η δυνατότητα σε απλούς χρήστες να διασφαλίσουν τα δεδομένα τους και μια ενδεχόμενη μεγάλη δαπάνη για να τα ανακτήσουν σε περίπτωση καταστροφής.

GENERALI

insurance quality
www.iqbrokers.gr

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

DRP Data Rescue Plan by GENERALI

Ποιους αφορά;

- Όλους όσους έχουν κρίσιμα δεδομένα (Videos, Φωτογραφίες, έγγραφα και οποιοδήποτε άλλο σημαντικό έγγραφο)
- Όλους τους τύπους εσωτερικών και εξωτερικών δίσκων
- Ελεύθερους επαγγελματίες, ιδιώτες, ιατρούς κλπ

Τί ασφαλίζει;

- Όλους τους τύπους υπολογιστών & Laptop
- Όλους τους τύπους εσωτερικών και εξωτερικών δίσκων

Τί καλύπτει;

- Οποιαδήποτε βλάβξ
- Όλο το κόστος διαδικασίας ανάκτησης δεδομένων αποκλειστικά στην TicTac Laboratories

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

DRP by GENERALI Data Rescue Plan

Πλεονεκτήματα

- Κόστος ασφάλισης μόλις 30€
- Διάρκεια 2 έτη ασφάλισης
- Απλότητα διαδικασίας απλή εγγραφή του χρήστη με τα στοιχεία του μέσου (σκληρός δίσκος) στο drp.gr
- Ξεκάθαροι όροι ασφάλισης
- Καινοτομία στον τρόπο καταγραφής των στοιχείων του δίσκου από το ειδικό λογισμικό που δημιουργήθηκε στο drp.gr

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Πραγματογνωμοσύνη σε Ψηφιακά Δεδομένα

Βρίσκουμε τις αποδείξεις που ψάχνετε

Αναζητάτε αποδείξεις σε κινητά τηλέφωνα ή σε ηλεκτρονικά αρχεία; Μπορούμε να βοηθήσουμε!

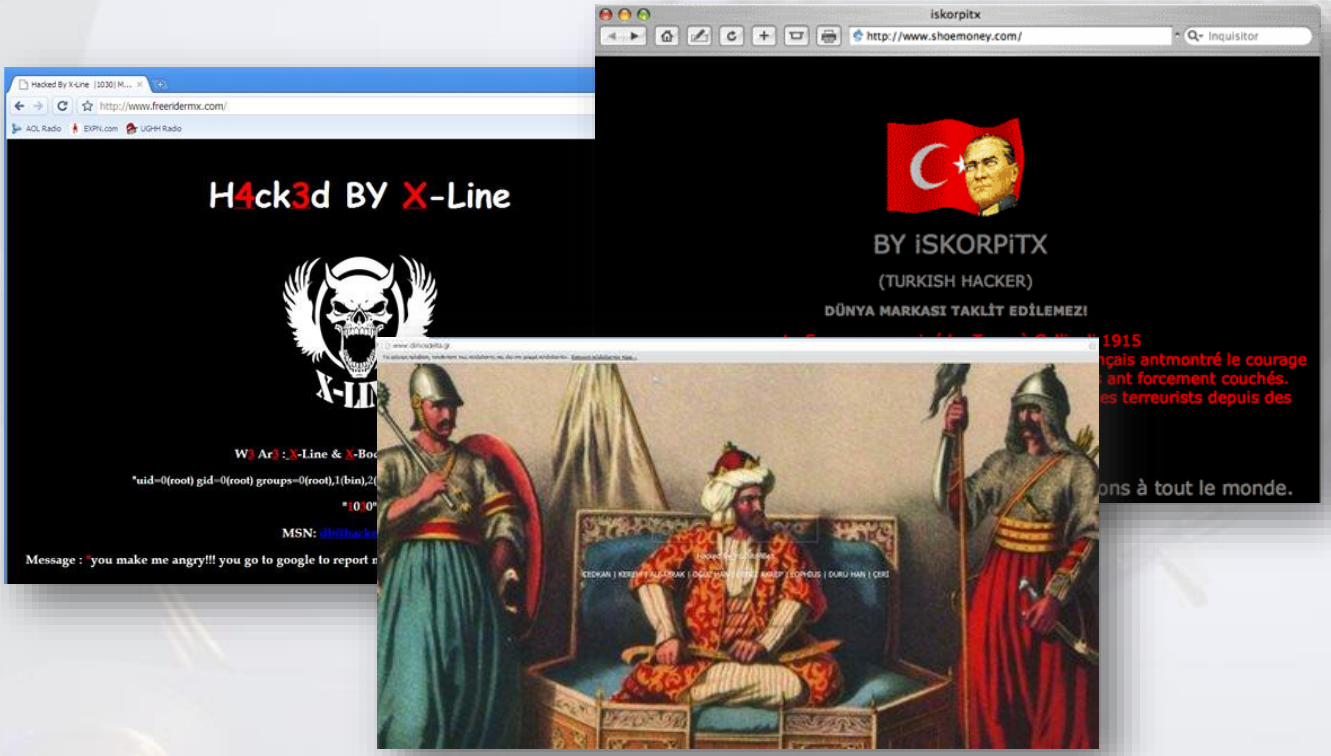
TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Δεδομένα στα σκουπίδια… κίνδυνος!
Πιστοποιημένη καταστροφή δεδομένων

Δεν μπορείτε να φανταστείτε πόσο πολύτιμα είναι για κάποιον τα… δεδομένα σας!

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Επίλυση προβλημάτων hacking
σε Wordpress & άλλα CMS



Πολλές φορές σε επιθέσεις από hackers, το να επαναφέρετε backup δεν βοηθάει γιατί οι hackers έχουν ήδη «εγκατασταθεί».
Αφαιρούμε τον κώδικα και σας προστατεύουμε.

TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Ευχαριστούμε

11 τρόποι προστασία από Ransomware - Whitepaper

Κατεβάστε το Free Report από την ιστοσελίδα :

http://tictac.gr/