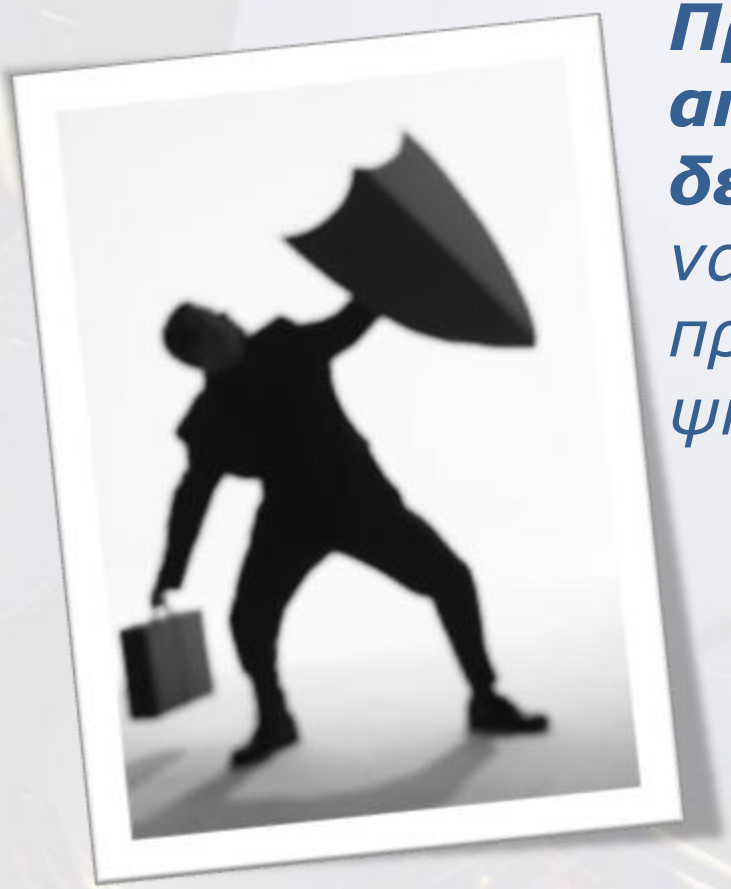
Δεδομένα υπό πολιορκία



Πραγματικά περιστατικά απώλειας & διαρροής δεδομένων *και πώς μπορείτε να προστατέψετε την προσωπική και την εταιρική σας ψηφιακή περιουσία*

Παναγιώτης Πιέρρος

Managing Director της
TicTac Data Recovery

Μιχάλης Μίγγος

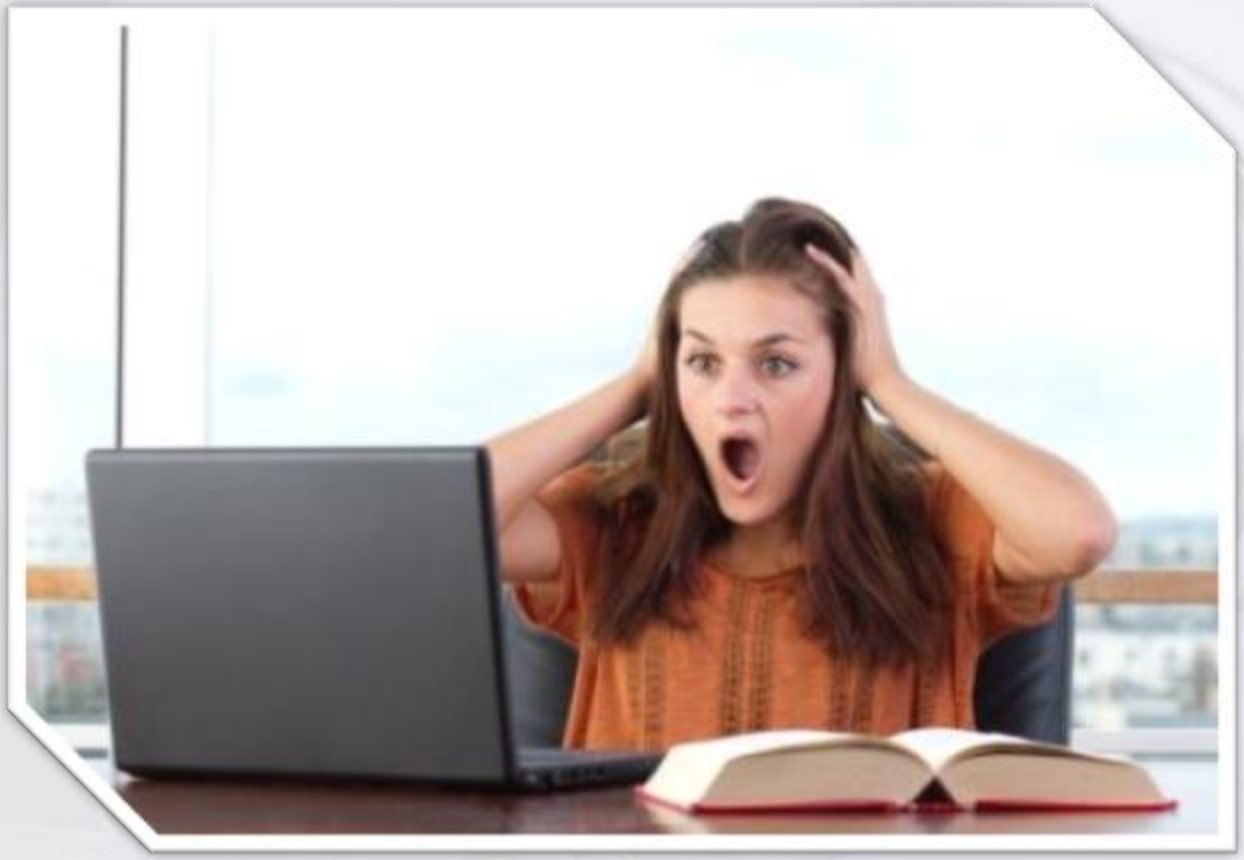
Technical Director της
TicTac Data Recovery

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

Μόλις τελειώσει αυτή η παρουσίαση θα είστε σε θέση να γνωρίζετε…

1. **Απώλεια Δεδομένων :** Πιθανοί **λόγοι απώλειας δεδομένων** και πως μπορούν να αντιμετωπιστούν
2. **Διαρροή Δεδομένων:** Τι πρέπει να γνωρίζεις πριν πετάξεις μια συσκευή που περιέχει δεδομένα
3. **Ransomware:** Λειτουργία, στατιστικά και αντιμετώπιση ιών όπως ο Cryptowall
4. **Ο Ανθρώπινος Παράγοντας:** Τι ζημιές μπορεί να προκαλέσει και πώς θα ανακαλύψουμε τι έχει συμβεί;
5. **Το Cloud:** Τι πρέπει να γνωρίζουμε και πότε προτείνουμε τη χρήση του;

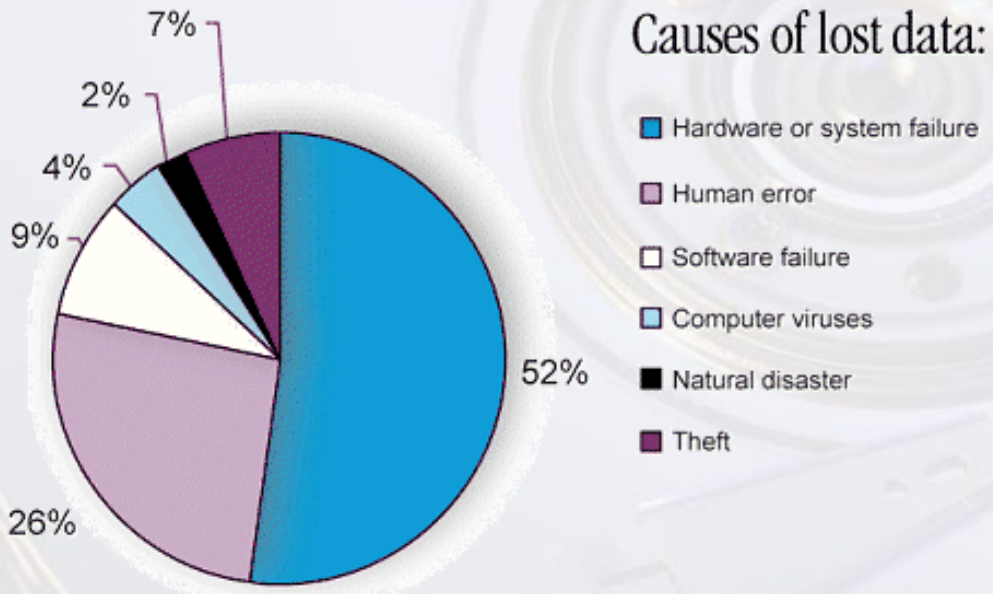
TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr



Απώλεια Δεδομένων

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

Στατιστικά Απώλειας δεδομένων



70% of businesses that suffer a major data loss are out of business within 18 months.

Source: DTI

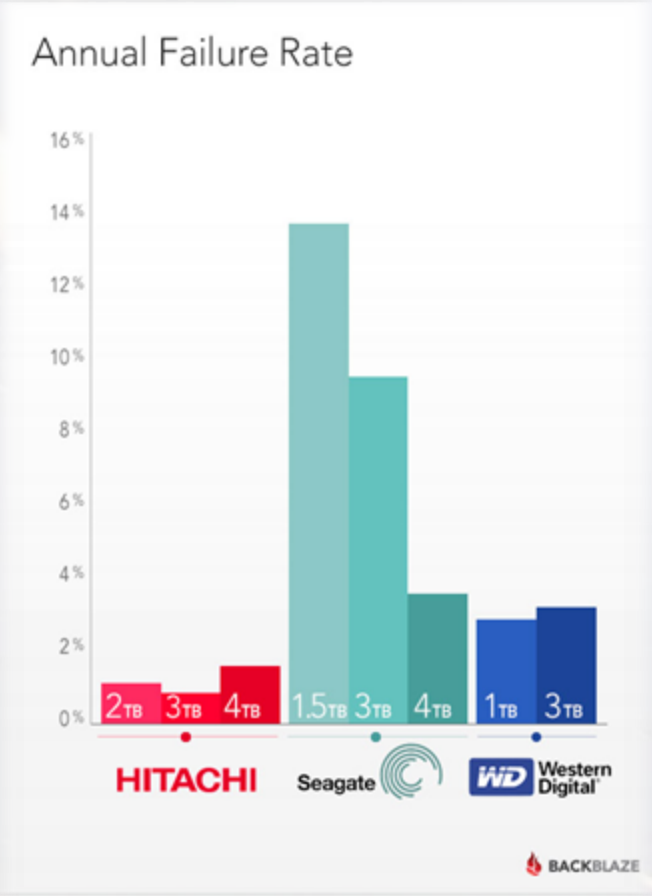
TICTAC LABORATORIES
DATA RECOVERY • COMPUTER FORENSICS
www.tictac.gr

Παραδείγματα Απειλών

- **Αστοχία Αποθηκευτικών μέσων**
  - Σκληροί δίσκοι, Raid συστήματα, USB Flash, SSD… όλα μπορεί να χαλάσουν
- Ανθρώπινο Λάθος
  - Ακούσια διαγραφή/μεταβολή/κακή χρήση/έλλειψη backup αρχείων
- Πρόβλημα στο Software
  - Προβλήματα στο Filesystem/στο λειτουργικό/στη βάση
- **Ιοί / Malware / Εξωτερικές επιθέσεις**
  - Cryptolocker/Ransomware
- Φυσικές Καταστροφές
  - Φωτιά/Πλημμύρα/Πτώσεις τάσης
- **Κλοπή/Δολιοφθορά**
  - Προσωπικό/Συνεργάτες
- **Απόσυρση του μέσου χωρίς ελεγχόμενες διαδικασίες**
  - Δωρεά/Μεταπώληση/Recycling

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

Στατιστικά από το εργαστήριο & συμπεράσματα



1. **5-10% των δίσκων παρουσιάζουν αστοχία υλικού στην 3ετία** (Ηλεκτρονικό / Μηχανικό πρόβλημα ή δυσλειτουργία στο Firmware)
2. Είδαμε δίσκους **3TB να χαλάνε 20-30 ημέρες** από την αγορά τους
3. Πολλοί **SSD δίσκοι συνάντησαν με ελαττωματικό firmware** και δεν κατάφερε η εταιρία να το διορθώσει ποτέ
4. Εκατοντάδες **επώνυμα USB Flash Disks σταμάτησαν να λειτουργούν ξαφνικά**
5. Σε **συστοιχίες Raid «χτύπησαν» ταυτόχρονα πολλαπλοί δίσκοι**
6. Όσοι μεγαλώνουν οι χωρητικότητες **αυξάνονται τα προβλήματα** και ο **όγκος των δεδομένων που χάνεται**
7. **6%** των υποθέσεων ήταν **μη ανακτήσιμες** όταν παραλάβαμε **λόγω επέμβασης (2014)**
8. **2%** των υποθέσεων **ήταν μη ανακτήσιμες.**

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 2014 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

Διαρροή Δεδομένων

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

Γνωρίζετε τι είναι αυτά;

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

Τα δεδομένα σας διαθέσιμα… στο κοινό!

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

Data στα σκουπίδια και στο ebay!

65% των μέσων αποσύρονται χωρίς να λάβει μέτρα ασφαλείας

Από **Dealer ανακυκλωμένων ηλεκτρονικών συσκευών**, αγοράστηκαν **100 σκληροί δίσκοι** οι οποίοι φαίνονταν εξωτερικά σε πολύ άσχημη κατάσταση:

- **Ανακτηθήκαν:** 57 δίσκοι, οι 44 ολικώς και οι 13 μερικώς
- **Βρέθηκαν:** Δεδομένα ιδιωτικών ή δημόσιων οργανισμών, εταιρικά & προσωπικά αρχεία

Αγοράσαμε 15 κινητά τηλέφωνα και 30 σκληρούς δίσκους από το eBay:

- **Στα κινητά:** βρέθηκαν προσωπικά ή εταιρικά δεδομένα σε **8 από αυτά**.
- **Στους δίσκους:** ανακτήθηκαν δεδομένα από 8 δίσκους.

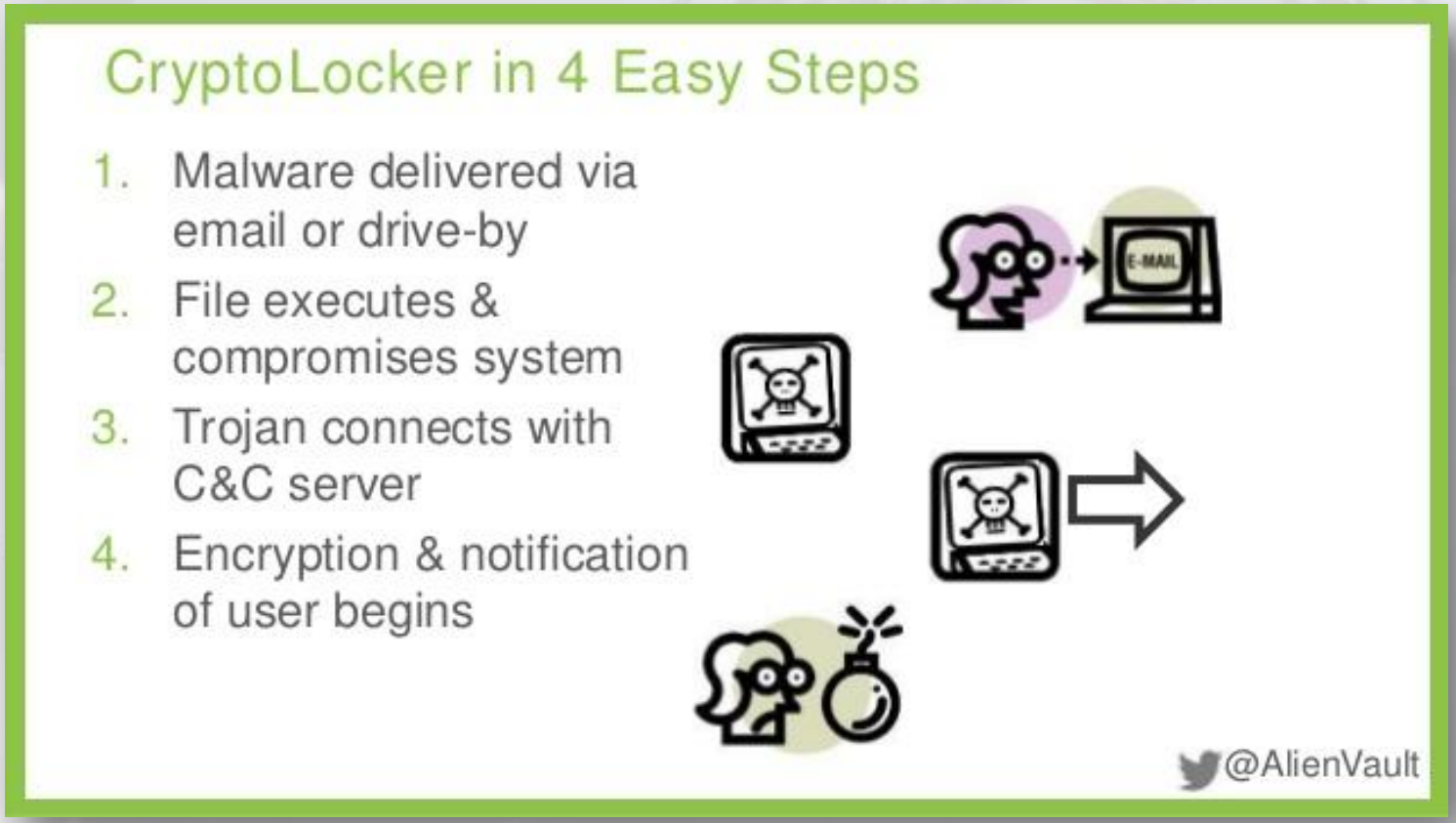
Λύση: Πιστοποιημένη διαγραφή δεδομένων

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

Ransomware: Ψηφιακός Εκβιασμός

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

Τι κάνει ένας ιός τύπου Cryptolocker;



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

https://kpai7ycr7jxqkilp.torexplorer.com/xxxx

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **12/05/14 - 21:37** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:

103h 37m 58s

Your system: Windows 7 (x64) First connect IP: 198.15.79.146 Total encrypted **56** files.

Refresh | Payment | FAQ | Decrypt 1 file for FREE | Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

bitcoin

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Recommended for fast, simple service.
- Coinbase - Bitcoin exchange based in the United States. (Highly rated).
- BitStamp - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
- CoinJar - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 1.22 BTC to Bitcoin address: 1BhLzCZGY6dwQYgX4B6NR5sjDebBPNapvv Get QR code

4. Enter the Transaction ID and select amount:

1.22 BTC ~= 500 USD | Clear

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

...e check the payment information and click "PAY".

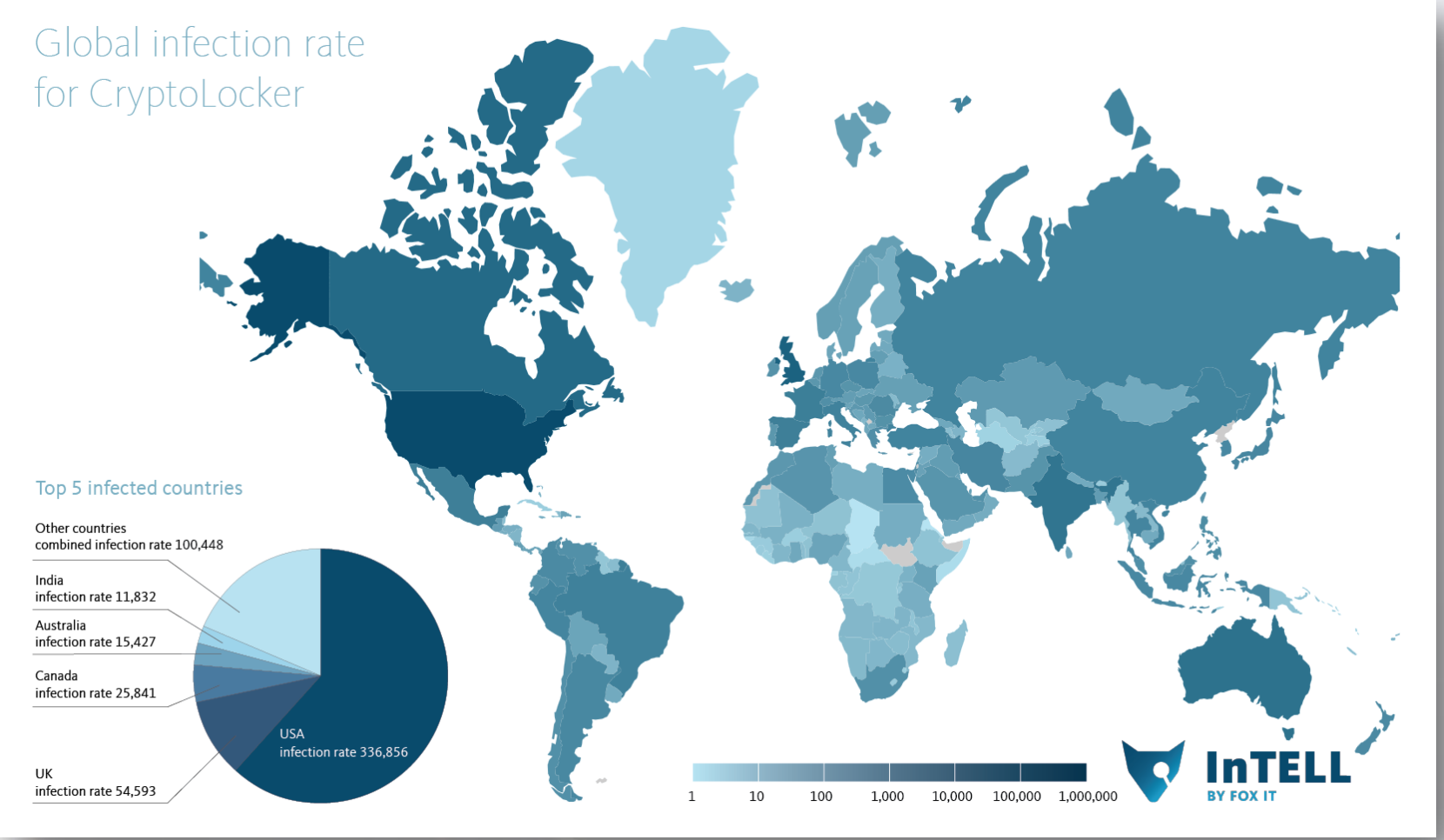
SpywareTechs.com

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

- Η πληρωμή των λίτρων μέσω **BitCoins/Moneypack** εξασφαλίζει ανωνυμία στον θύτη αλλά **δεν εξασφαλίζει 100% εγγυημένη ανάκτηση**

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

Ο Χάρτης μόλυνσης από Cryptolocker



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

Υπάρχει ελπίδα;

Ποια είναι τα δεδομένα;

- **Δεν υπάρχει επίσημη λύση για 100% ανάκτηση ακόμα**, αν και παρακολουθούμε στενά το θέμα
- Υπάρχουν κάποιες **δοκιμαστικές προσπάθειες**
- Σε **18%** των υποθέσεων καταφέραμε **ολική ανάκτηση των ζητούμενων αρχείων**
- Σε **41%** καταφέραμε **μερική ανάκτηση των αρχείων**
- **Pro-Active:** Backup με versioning & Updated Antivirus
- **Περισσότερες πληροφορίες:** http://tictac.gr/cryptolocker-notepad

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

Ο Ανθρώπινος Παράγοντας

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

Δολιοφθορές… εκ των έσω…

Μπορούμε να προβλέψουμε πολλά όσον αφορά την απώλεια ή την αλλοίωση των δεδομένων… αλλά δύσκολα προβλέπουμε τον παράγοντα άνθρωπο!

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

Κακόβουλες ενέργειες

- Χρήση του εταιρικού δικτύου ή Server για παράνομες ενέργειες
- Διακίνηση εταιρικών δεδομένων
- Παραποίηση εταιρικών δεδομένων
- Πρόσβαση σε διαβαθμισμένα έγγραφα από μη εξουσιοδοτημένο προσωπικό
- Κατασκοπεία
- Δολιοφθορά
- Κλοπή Ψηφιακής Ταυτότητας
- Παράνομες Ενέργειες στα Social Media
- Παράνομες συνομιλίες
- Κατοχή παράνομου υλικού

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

Digital Forensics :
Πραγματογνωμοσύνη σε Ψηφιακά Δεδομένα

Αφού γίνει μια δολιοφθορά, πλέον η τεχνολογία μας βοηθάει να εξάγουμε αρκετά στοιχεία κατόπιν ψηφιακής έρευνας

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

Στατιστικά ερευνών μέσα στο 2014

Κάποια από τα περιστατικά που είδαμε:

- 33% περιστατικά **δολιοφθοράς υπαλλήλων σε εταιρικά αρχεία**, τα περισσότερα έγιναν κατά την παύση συνεργασίας του υπαλλήλου με την εταιρία
- Αρκετά περιστατικά **δολιοφθοράς ή παραποίησης αρχείων** από τους ίδιους τους μετόχους
- Μερικά περιστατικά αφορούσαν Παραποίηση λογιστικών ή οικονομικών αναφορών
- Απόκρυψη περιουσιακών στοιχείων

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

Το Cloud και τα δεδομένα σας

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

Backup σε τοπικά μέσα

- **ΚΟΣΤΟΣ:** Το κόστος ανα 1TB Cloud είναι περίπου 100$/έτος, ενώ αγοράζει κάποιος ένα εξωτερικό δίσκο με 1TB με 100$ για πάντα.
- **ΙΔΙΩΤΙΚΟΤΗΤΑ:** Στο Cloud τα δεδομένα μας είναι αλλού
- **ΦΟΡΗΤΟΤΗΤΑ:** Ένα εξωτερικό Drive μεταφέρεται παντού
- **ΑΣΦΑΛΕΙΑ**: Ένα εξωτερικό drive μπορεί να κρυπτογραφηθεί για μέγιστη ασφάλεια
- **ΤΟ ΔΙΚΟ ΣΟΥ CLOUD:** Είναι εφικτό πλέον μέσω Software

- **ΑΣΤΟΧΙΑ ΥΛΙΚΟΥ:** Οι σκληροί δίσκοι χαλάνε σε οποιαδήποτε μορφή τους. Η ασφαλέστερη λύση είναι διπλή αποθήκευση. Οι εταιρίες δίνουν εγγύηση αλλά όχι για τα Data!
- **ΥΠΕΥΘΥΝΟΤΗΤΑ ΓΙΑ BACKUP**: Έχετε όλη την ευθύνη σε περίπτωση απώλειας.

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

Backup στο Cloud

- **BACKUP**: Εξασφαλισμένο και Worry Free Backup / Restore
- **ΕΠΕΚΤΑΣΙΜΟΤΗΤΑ**: Πληρώνεις και αναβαθμίζεις κατά βούληση & χωρίς διαδικασίες
- **ΑΜΕΣΟΤΗΤΑ**: Τα δεδομένα σας βρίσκονται σε Servers με πολύ καλές ταχύτητες και άμεσα διαθέσιμα
- **ΣΥΓΧΡΟΝΙΣΜΟΣ**: Πολλές συσκευές, ένας κεντρικός χώρος διαχείρισης
- **ΕΥΚΟΛΙΑ**: Γρήγορο Setup και λειτουργία

- **ΚΟΣΤΟΣ:** Υψηλό κόστος σε σχέση με το τοπικό Hardware
- **ΙΔΙΩΤΙΚΟΤΗΤΑ**: Τίθεται μεγάλο ερώτημα για την ασφάλεια και την ιδιωτικότητα δεδομένων που έχουμε σε εγκαταστάσεις τρίτων.

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

Το υβριδικό μου Cloud

Έχει όλα τα καλά του Cloud χωρίς τα περισσότερα μειονεκτήματα του

Πληροφορίες στο Stand της TicTac…

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

Ευχαριστούμε

Πόσο αξιόπιστοι είναι οι σκληροί δίσκοι σήμερα;

Κατεβάστε το Free Report από την ιστοσελίδα :
http://tictac.gr/hard-disk-failure-report-2014

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