Παναγιώτης Πιέρρος
GENERAL MANAGER
Tictaclabs Cyber Security

Μιχάλης Μίγγος
TECHNICAL DIRECTOR
Tictaclabs Cyber Security

ΠΑΡΑΣΚΕΥΗ
Η καλύτερη ημέρα για Ransomware

Εμπειρίες από το Thriller των Επιχειρήσεων με τα Ransomware

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Ανάκτηση Δεδομένων

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

ΣΚΑΡΛΟΣ

Managed Backup & Disaster Recovery

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Managed Cyber Security Services (MSSP)

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

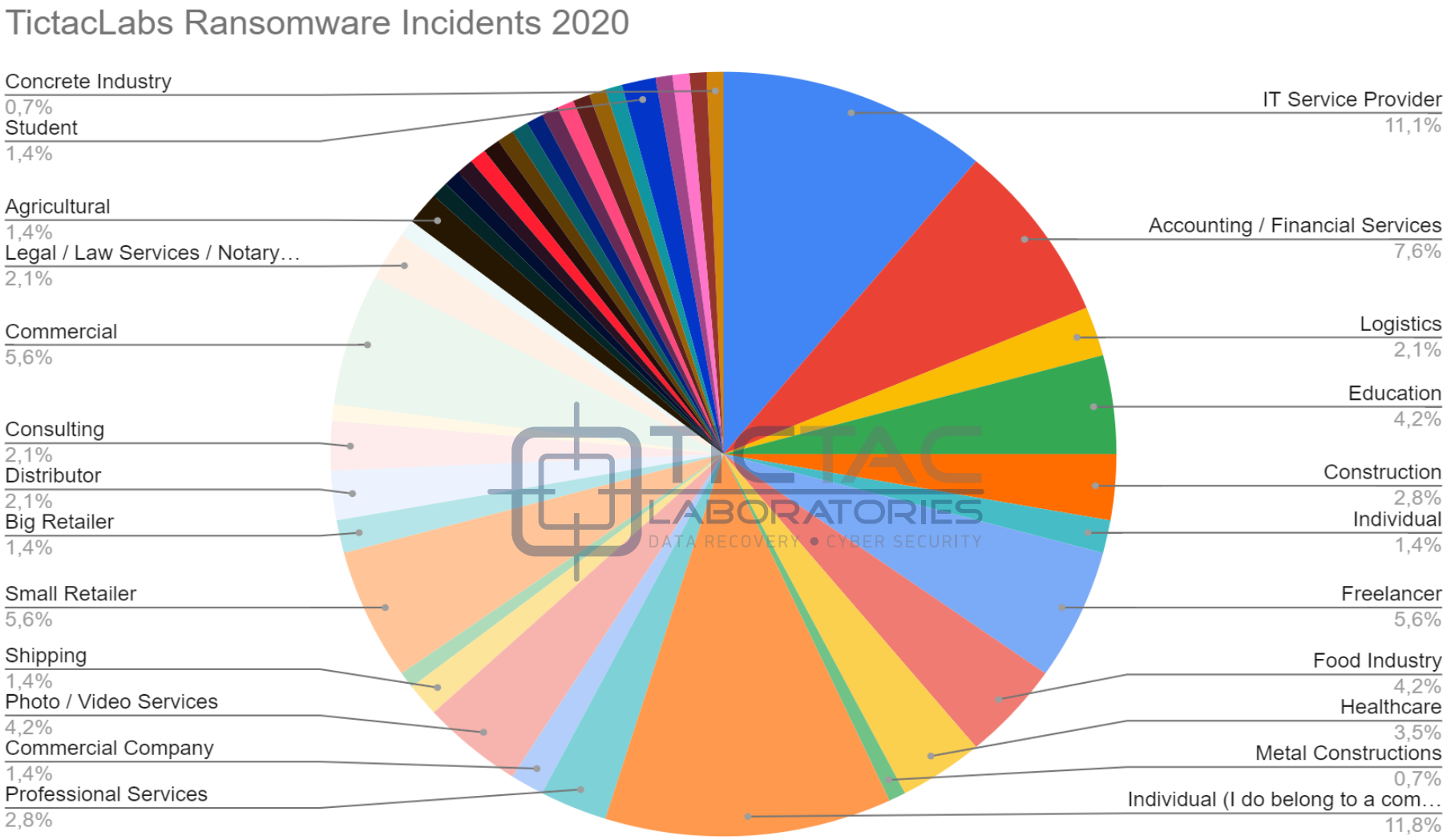
Tictac Ransomware Stats 2020

Ψηφιακά Λύτρα, Στατιστικά και Τρόποι Προστασίας

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Copyright 2018 @ Tictac Data Recovery

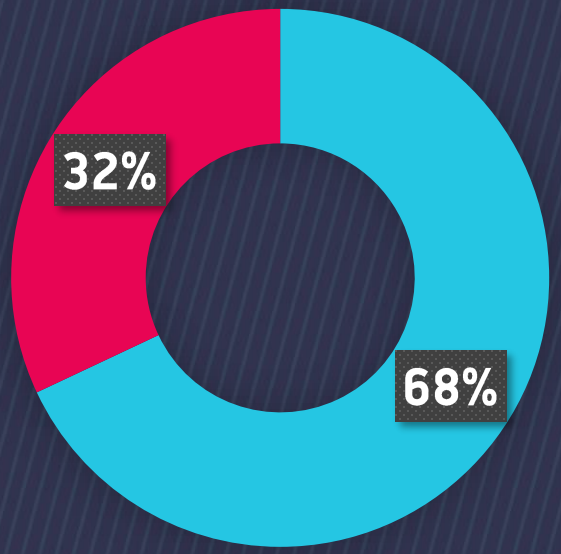
Κλάδοι που έχουν χτυπηθεί περισσότερο το 2020



Οικογένειες Ransomware
που κυριάρχησαν το 2021

Τεχνική Υποδομή των πληγέντων 2019

Τεχνικό Τμήμα

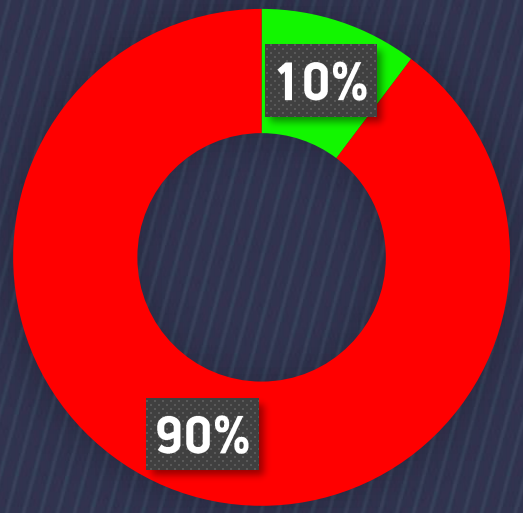


ΕΞΩΤΕΡΙΚΟ ΕΣΩΤΕΡΙΚΟ

Μέσος όρος Workstations

9.4

Το backup λειτούργησε;



ΝΑΙ ΟΧΙ

Πραγματικά κόστη μιας επίθεσης Ransomware

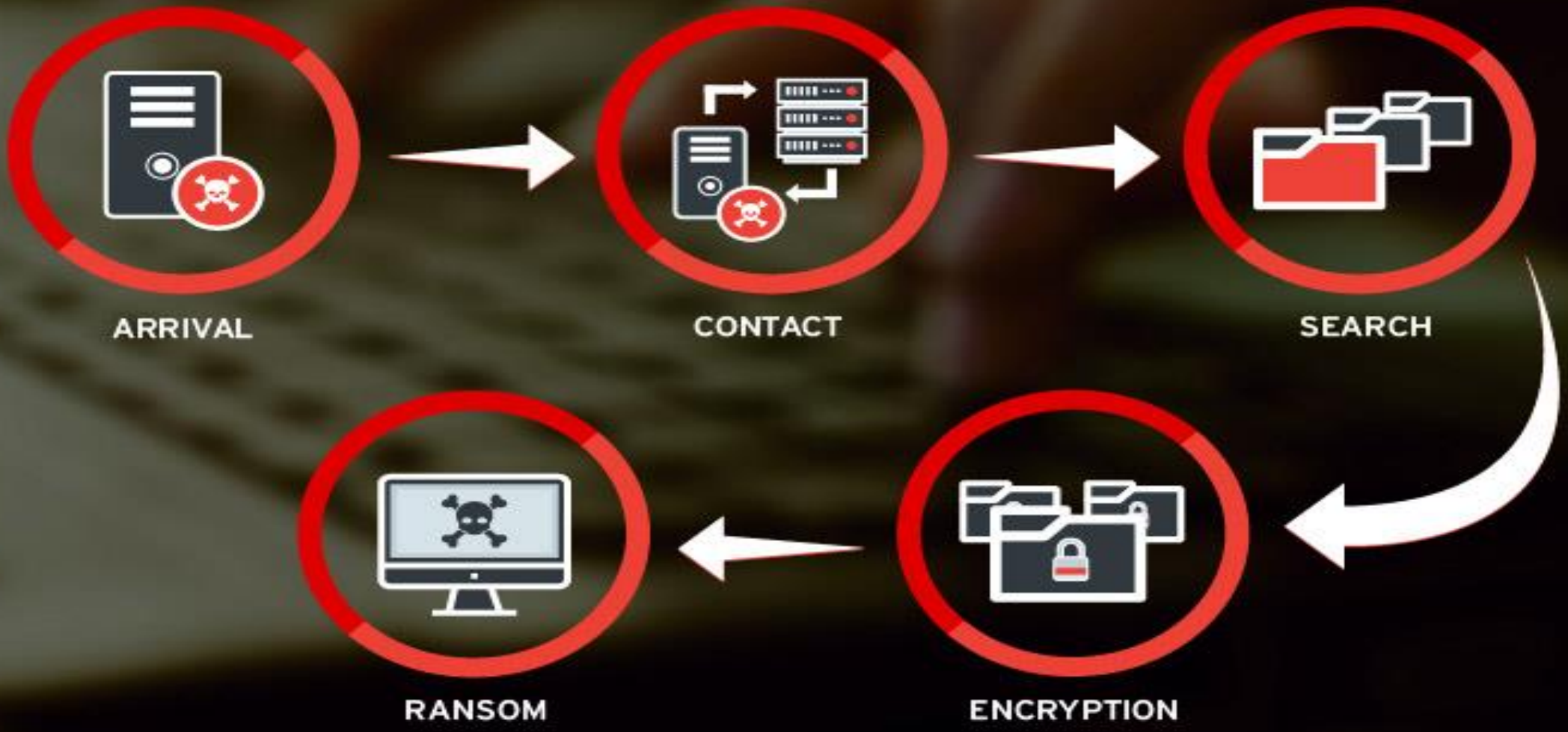
Μέσος χρόνος διάρκειας περιστατικού	Μέσο κόστος Επαναφοράς Δεδομένων	Μέσο Κόστος Προσωρινής Διακοπής Εργασιών Εταιρίας
7.4 μέρες	12.193 ευρώ	31.321 ευρώ

- Ο Μέσος χρόνος διάρκειας περιστατικού υπολογίζεται είτε η εταιρία στήσει από την αρχή την υποδομή της είτε πληρώσει τα λύτρα
- Η Συνολική Δαπάνη περιλαμβάνει έξοδα Μηχανογράφου, Εξειδικευμένου Συμβούλου Ransomware, Λύτρων κλπ
- Δεν έχουν υπολογιστεί πιθανά διοικητικά πρόστιμα από την Αρχή Προστασίας Δεδομένων & άλλους φορείς

RANSOMWARE

BEHIND THE SCENES

By the time victims see the ransom note, it's already too late—ransomware has already encrypted files before they know it's there.
Here's what happens between infection and the ransom demand.



Τα Trends των περιστατικών ασφαλείας το 2021

Αύξηση στα Ransomware και κυρίως στα ποσά:

- Ιδιώτες: 500$ - 3000$
- Επιχειρήσεις 2-3 υπολογιστών: 3000$ - 8.000$
- Επιχειρήσεις έως 20-30 υπολογιστών: 20.000$ - 50.000$
- Μεγάλοι Οργανισμοί: 100.000$ - 50.000.000$

Είδαμε να ακολουθεί 2η επίθεση Ransomware να ακολουθεί αμέσως μετά την πρώτη. Credentials @ Risk

Είχαμε πάνω από 15 περιστατικά με διπλή κρυπτογράφηση

Είχαμε περιστατικά όπου η αποκρυπτογράφηση δεν λειτούργησε σωστά και χρειάστηκε πολύ ειδικός χειρισμός για να αποκρυπτογραφήσουμε τα μεγάλα αρχεία.

Μέσω των διαδικασιών Computer Forensics διαπιστώσαμε:

- Περιστατικά όπου ο επιτιθέμενος ήταν μέσα στην υποδομή για πάνω από 2 μήνες χωρίς να γίνει αντιληπτός
- Ο επιτιθέμενος έκανε Corrupt τα Offline backups και μετά έκανε την κρυπτογράφηση
- Ο επιτιθέμενος είχε Domain Admin Access και μπορούσε να απεγκαταστήσει τα εργαλεία προστασίας όποτε επιθυμούσε

Εκατοντάδες υποθέσεις Business Email Compromise SCAM (BEC SCAM)

Πολλές υποθέσεις με Οικονομικές απάτες, Forex Scams

Υποθέσεις κλοπής κρυπτονομισμάτων (New)

Ransomware Incident Response

Οι περισσότερες εταιρίες αψηφούν τον κίνδυνο

Δεν γνωρίζουμε
τις αδυναμίες μας

Τί γίνεται όταν έχουμε Ransomware σε έναν Οργανισμό;

- Τα δεδομένα δεν είναι διαθέσιμα
- Διακοπή λειτουργίας του οργανισμού
- Οικονομικές απώλειες ξεκινάνε από την πρώτη ημέρα και δεν γνωρίζουμε πότε θα τελειώσει
- Νομικές Συνέπειες για διαρροές δεδομένων
- Ένα κακόβουλο τρίτο άτομο είχε πρόσβαση στο δίκτυο
- Συνέπειες προς τρίτα μέρη
- Πιθανή διαρροή δεδομένων
- Επικρατή σύγχυση και πανικός τόσο στο τεχνικό τμήμα όσο και στη διεύθυνση
- Δεν σκεφτόμαστε με λογική
- Δεν γνωρίζουμε τίποτα για τον αόρατο εχθρό

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Πού μπορούμε να βοηθήσουμε σε μια επίθεση Ransomware;

Κάθε χρόνο διαχειριζόμαστε εκατοντάδες περιστατικά σε όλο τον κόσμο με στόχο:

- Γρήγορη επαναφορά των αρχείων
- Γρήγορη επαναφορά λειτουργίας του Οργανισμού με ασφάλεια
- Μείωση των λύτρων
- Συντονισμός Διεύθυνσης και IT Τμήματος
- Ενημέρωση περί νομικών ζητημάτων και διαδικασιών
- Διερεύνηση του πώς προέκυψε η μόλυνση (πόσο ήταν ο Hacker μέσα, τι υπέκλεψε, από που ξεκίνησε, βρίσκεται ακόμα μέσα στην υποδομή)
- Υποβοήθηση σε διαδικασίες Κρυπτονομισμάτων
- Συμβουλευτική στην μελλοντική ασφάλεια του οργανισμού

Συμβουλές από ένα Hacker

Τι πρέπει να γνωρίζουμε

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

From your hacker with Love…

1. buy paid antivirus
2. don’t use user account "administrator" on other hosts than controller domain.
3. set all users "users" privileges

… find out the rest at www.tictac.gr/love-hacker

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

http://www.tictac.gr/love-hacker

…this text is just copy paste from a real incident.

Το μεγαλύτερο λάθος που έκανα είναι, ότι ενώ η επιχείρηση μου μεγάλωσε 3 φορές σε τζίρο τα τελευταία χρόνια, δεν αύξησα αντίστοιχα το budget στο IT Department / Cyber Security.

CEO γνωστής Ελληνικής Εταιρίας που έπεσε θύμα Ransomware

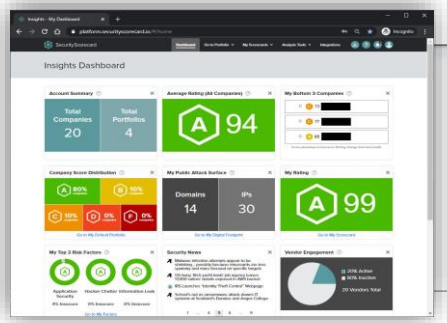
3 Workshops Tictac:
Λύσεις Προστασίας από Ransomware

Πώς περιορίζουμε μια επίθεση Ransomware

Παρασκευή 23/4/2021
11:30 - 12:15

Παρασκευή: 23/4/2021
13:00 - 13:45

Anti Ransomware Backup & Recovery



SecurityScorecard «Τι βλέπει ένας Hacker για εμάς;»

Παρασκευή 23/4/2021
15:15 – 16:00

Εγγραφές: www.tictac.gr/infocom2021

Το Cybercheck.gr είναι ο πρώτος ιστότοπος που παρέχει άμεση και δωρεάν πληροφορία για το επίπεδο κυβερνοασφάλειας ή ασφάλειας υποδομών και δεδομένων της επιχείρησής σας.

Μέσω της μεγάλης εμπειρίας της ομάδας της Tictac Data Recovery & Cyber security, παρέχουμε την δυνατότητα σε όλες τις επιχείρησεις εναξαρτήτως μεγέθους να έχουν ένα πρώτο συμπέρασμα για την κατάσταση κυβερνοασφάλειας τους, μετά από 3-5 λεπτά απαντώντας σε ερωτήσεις.

Μέσα από το cybercheck.gr, θα κάνετε ένα πρώτο έλεγχο στην επιχείρησή σας και θα λάβετε ένα προσωποποιημένο πλάνο δράσης και άμυνας (cyber plan).

Επόμενο

Δωρεάν Τεστ Cyber Security: www.cybercheck.gr

We take your data seriously!

Data Recovery since 1999

www.tictac.gr

Managed Cyber Security & Disaster Recovery

www.tictaclabs.com