“The GhostBusters”

Πώς προστατευόμαστε από έναν αόρατο εχθρό πριν είναι πολύ αργά;

Παναγιώτης Πιέρρος

GENERAL MANAGER
Tictac Cyber Security

Μιχάλης Μίγγος

TECHNICAL DIRECTOR
Tictac Cyber Security

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Τι ομοιότητες έχουμε με τους Ghostbusters

Είμαστε μια ομάδα με εξειδικευμένη γνώση και αντιλαμβανόμαστε τον εχθρό που δεν είναι ορατός με γυμνό μάτι

Χρησιμοποιούμε πολύ εξειδικευμένα εργαλεία για τον εντοπισμό του εχθρού όσο και για την αποτροπή της επίθεσης

Επεμβαίνουμε σε πολύ δύσκολες καταστάσεις

«Καθαρίζουμε» γρήγορα και αποτελεσματικά

Ο εχθρός μπορεί να προκαλέσει πολύ μεγάλη καταστροφή αν δεν τον περιορίσουμε γρήγορα

Ενημερώνουμε στα συνέδρια ότι ο εχθρός υπάρχει, αλλά κανείς δεν μας πιστεύει μέχρι που έχει γίνει το κακό


RANSOMWARE ATTACK
You only have 3 days to submit the payment, or your files will be lost.
Time Left
02:23:59:06

Tictac Cyber Threats Warning for 2022

Οι ψηφιακοί εγκληματίες στρέφονται και σε άτομα πέρα από εταιρίες

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Ransomware is inevitable

According to a another independent research project, the 2022 Data Protection Trends report, **76%** of the **3,393** surveyed organizations suffered at least one ransomware attack, while **24%** either avoided attacks or **were unaware** that an attack occurred.

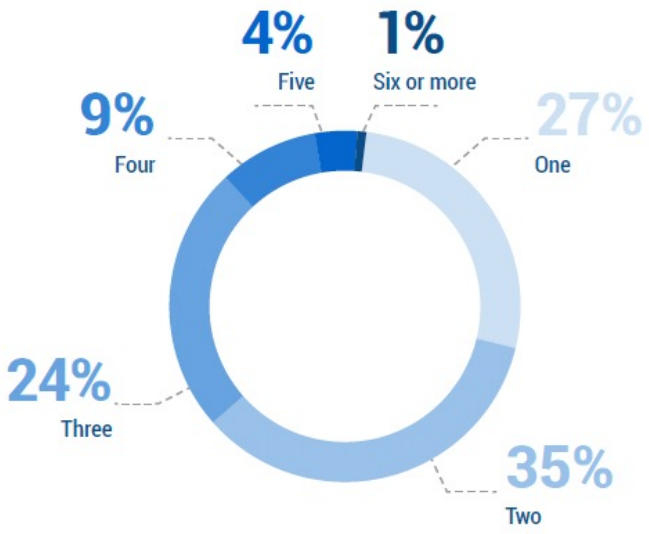
Organizations responding to this independent survey must have experienced at least one ransomware attack in 2021, revealing at least two important truths:

- Only about one in four (**27%**) organizations suffered just one attack, presumably with bad actors attempting to return for more ransom.
- Organizations of all sizes appear relatively equal in the persistence of attacks from small-to-medium-sized businesses (SMBs) (**100–249** employees) to large enterprises (**>5,000** employees). Said another way, just like any other disaster (fire/flood), ransomware attacks are universally pervasive.

While not charted, respondents to this survey reported an average of **47%** of their data being encrypted by ransomware.

This should scare every IT leader!

Figure 1.1 How many ransomware attacks has your organization suffered in the last 12 months? (n=998)



The most common entry point for a cyber attack is still phishing emails, malicious links, or a website that has dubious underpinnings. In considering the old mantra, "go with what works" it is unfortunate that even in 2022 with all the global awareness of ransomware and corporate training available, this is still the leading cause.

That said, there is plenty that IT professionals can do through increased diligence in patch-testing, credential management, role-based controls, etc. As a positive, only **1%** of respondents stated that they were not able to identify the entry-point; inferring that there have been improvements in monitoring and investigation tools across the security stack, as well as overall ransomware prevention strategies.

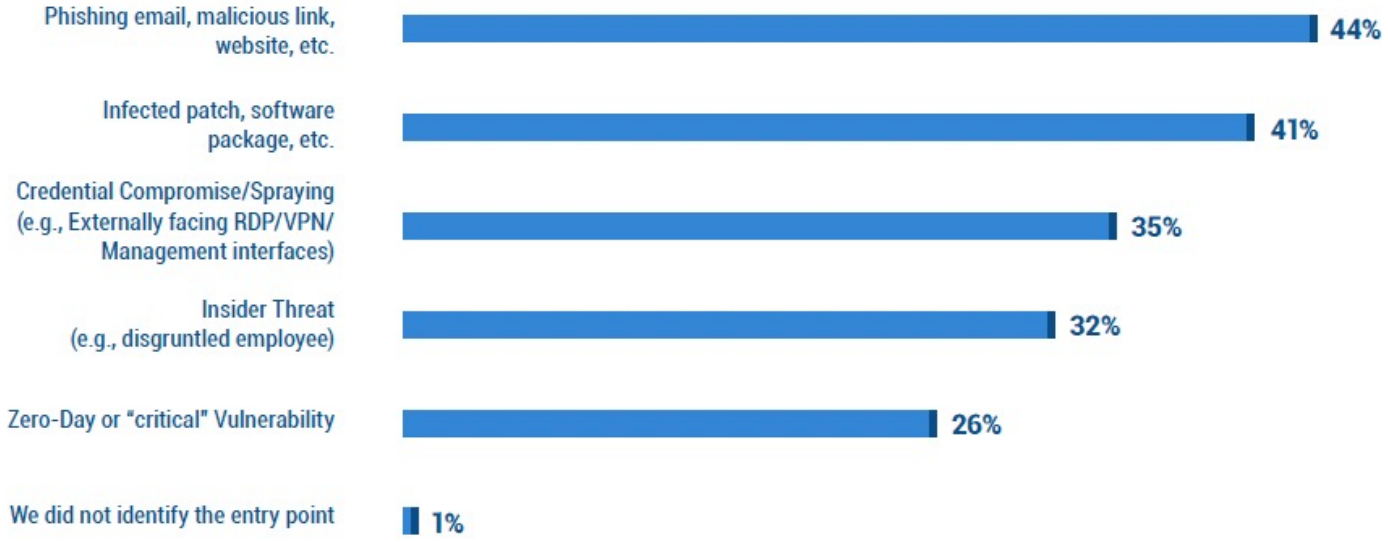
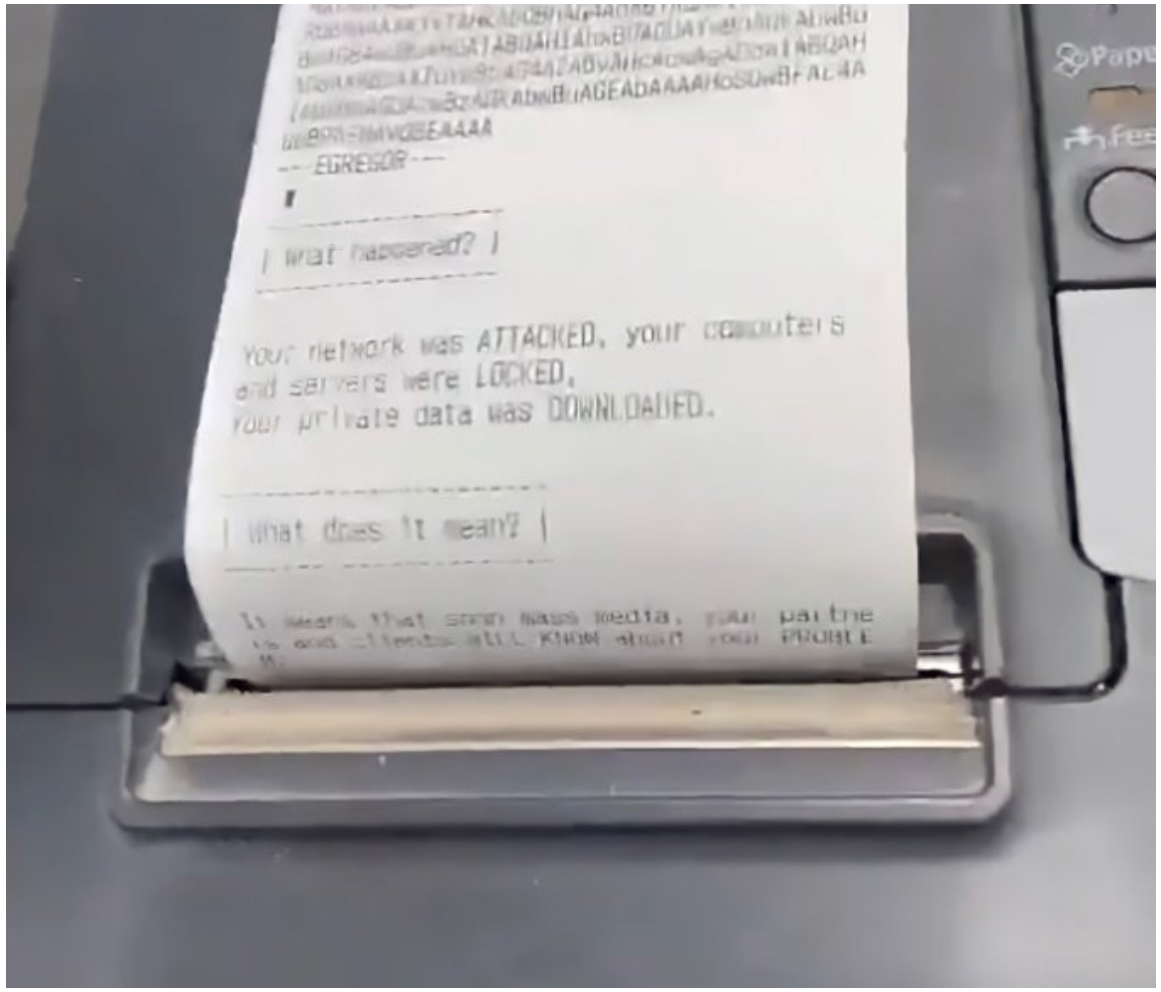
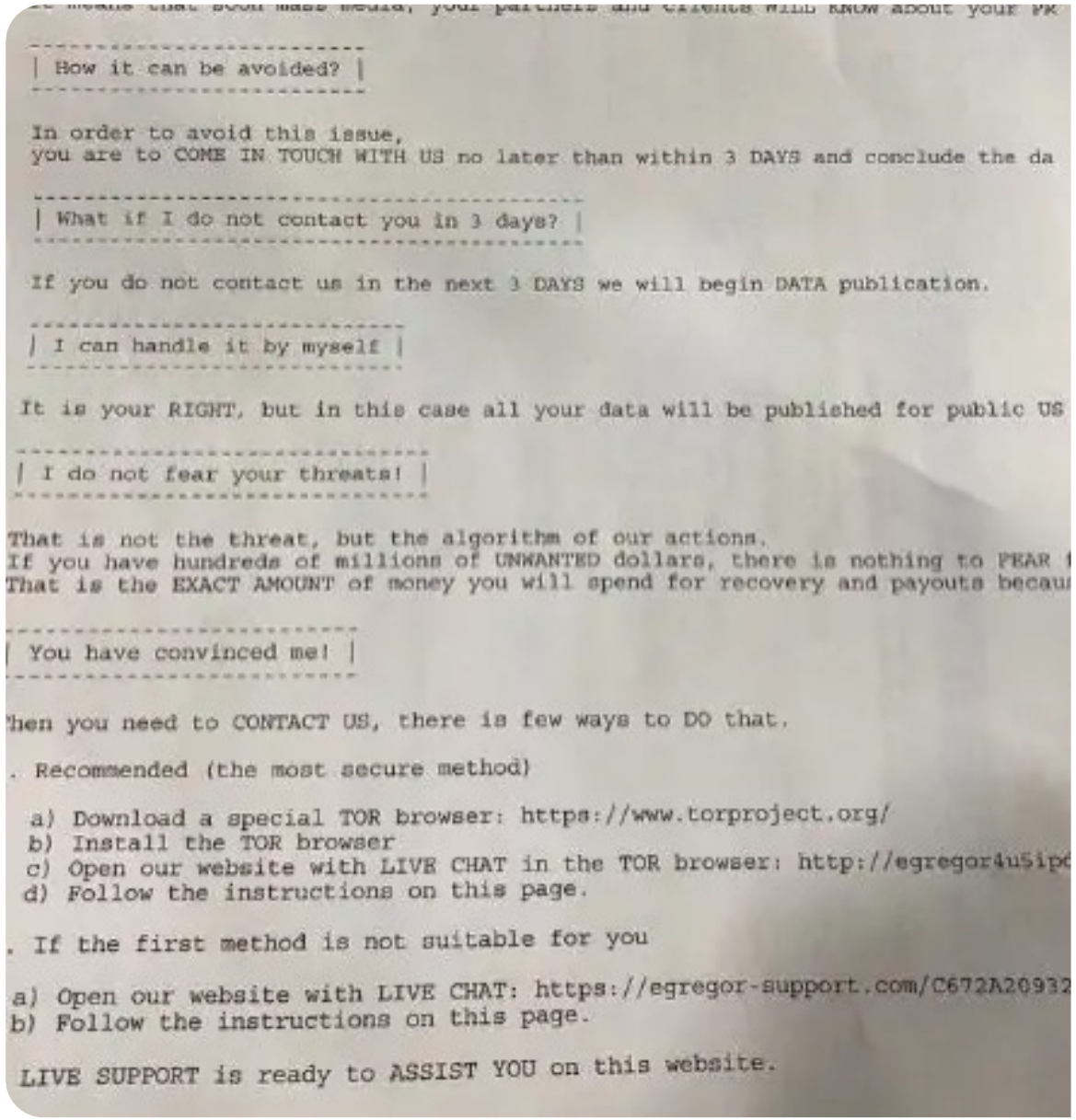


Figure 1.2 How did ransomware enter your organization's IT environment? (n=1,000)

Ransomware prints out the note

Έτσι γνωρίζουν και οι υπάλληλοι τι έχει συμβεί





| How it can be avoided? |

In order to avoid this issue,
you are to COME IN TOUCH WITH US no later than within 3 DAYS and conclude the da

| What if I do not contact you in 3 days? |

If you do not contact us in the next 3 DAYS we will begin DATA publication.

| I can handle it by myself |

It is your RIGHT, but in this case all your data will be published for public US

| I do not fear your threats! |

That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR
That is the EXACT AMOUNT of money you will spend for recovery and payouts becau

| You have convinced me! |

hen you need to CONTACT US, there is few ways to DO that.

. Recommended (the most secure method)

a) Download a special TOR browser: https://www.torproject.org/
b) Install the TOR browser
c) Open our website with LIVE CHAT in the TOR browser: http://egregor4u5ip
d) Follow the instructions on this page.

. If the first method is not suitable for you

a) Open our website with LIVE CHAT: https://egregor-support.com/C672A20932
b) Follow the instructions on this page.

LIVE SUPPORT is ready to ASSIST YOU on this website.


Facebook

energy_hashminer

55
Posts

12.7K
Followers

Leon Ellis
Bitcoin Mining Rig
☝️ Follow To Learn Trade Profit
📉 Foreign Exchange Trader
📚 Financial Education Mentor... more
[redacted].com

Follow

Messa

rayparisi 1

1,640
Posts

4,704
Followers

Ray Parisi
Storyteller, tequila drinker, luxe hunter, NYU
Executive Producer/Writer @CNBC 📺🎬@(
link in bio 👇 i know you want to tap that 😉
lnk.bio/Rays_Stories

Edit Profile

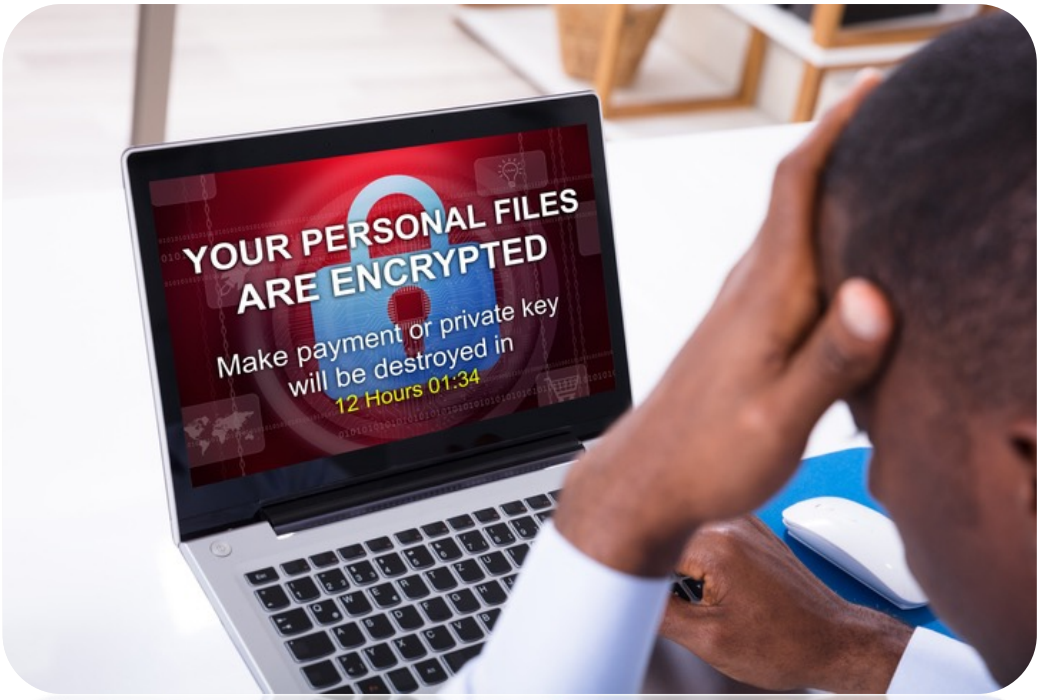
P

Τί γίνεται όταν έχουμε Κυβερνοεπίθεση 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
- Επικρατεί 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 Κυβερνοεπίθεση;



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

- Γρήγορη επαναφορά των αρχείων (όταν είναι εφικτό)
- Γρήγορη επαναφορά λειτουργίας του Οργανισμού με ασφάλεια (όταν είναι εφικτό)
- Μείωση των λύτρων μέσω διαπραγματεύσεων
- 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

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY


CYBER SECURITY

Τι είναι ένας MSSP ?

MSSP σημαίνει Managed Security Services Provider

Ο Ρόλος του MSSP είναι να φροντίζει μεταξύ άλλων:

- Την Ιδιωτικότητα , την Ακεραιότητα & την Διαθεσιμότητα των κρίσιμων αρχείων της υποδομής
- Συμβουλευτική Υποστήριξη στο IT Support τμήμα για θέματα ασφαλείας και προτάσεις βελτίωσης
- 24/7/365 εποπτεία του οργανισμού για θέματα ασφαλείας
- Εκπαίδευση του προσωπικού για θέματα ασφαλείας
- Διαχείριση οποιοδήποτε συμβάντος Ασφαλείας
- Υποβοήθηση για την εναρμόνιση του οργανισμού με τα διεθνή πρότυπα (NIST, HIPAA, GDPR κλπ)
- Δημιουργία αναφορών προς τη διοίκηση

Οι βασικές παροχές ενός MSSP

1. **Προστασία των τερματικών (Endpoint protection)**
   Antivirus Databases, Unknown file protection, Sandbox for Unknown files
2. **Προστασία των δεδομένων**
   Ransomware proof Automated Backup & Disaster Recovery with Cloud
3. **Προστασία του δικτύου**
   24/7/365 Firewall monitoring
4. **Κέντρο διαχείρισης συμβάντων ασφαλείας (SOC)**
   24/7/365 security monitoring από ανθρώπινο δυναμικό με ειδικά εργαλεία
5. **Διερεύνηση ηλεκτρονικών πειστηρίων Live**
   Digital Forensics σε περίπτωση εντοπισμού ανωμαλίας στο δίκτυο
6. **Cyber Security Insurance**
   Επειδή η κυβερνοασφάλεια είναι δύσκολο να εγγυηθεί 100%
7. **Cyber Security Awareness και εκπαίδευση**
   Εκπαιδεύουμε το προσωπικό μας για να γνωρίζει τι να περιμένει

Διαχειριζόμαστε την ασφάλεια του δικτύου και της υποδομής σας, ώστε να εστιάσετε στην εργασία σας

3 Workshops Tictac:
Λύσεις Προστασίας από Κυβερνοεπιθέσεις

How to setup your Disaster Recovery in a box with Acronis

Τετάρτη 6/7/2022
14:30 – 15:00

Τετάρτη 6/7/2022
15:00 – 15:30

Say bye bye to physical Servers and simplify your life with Infrastructure as a Service

Zero Trust with an EDR that grants IT Superpowers

Τετάρτη 6/7/2022
15:30 – 16:00

Γραφτείτε εδώ: https://tictac.gr/recommends/infocom2022/

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).

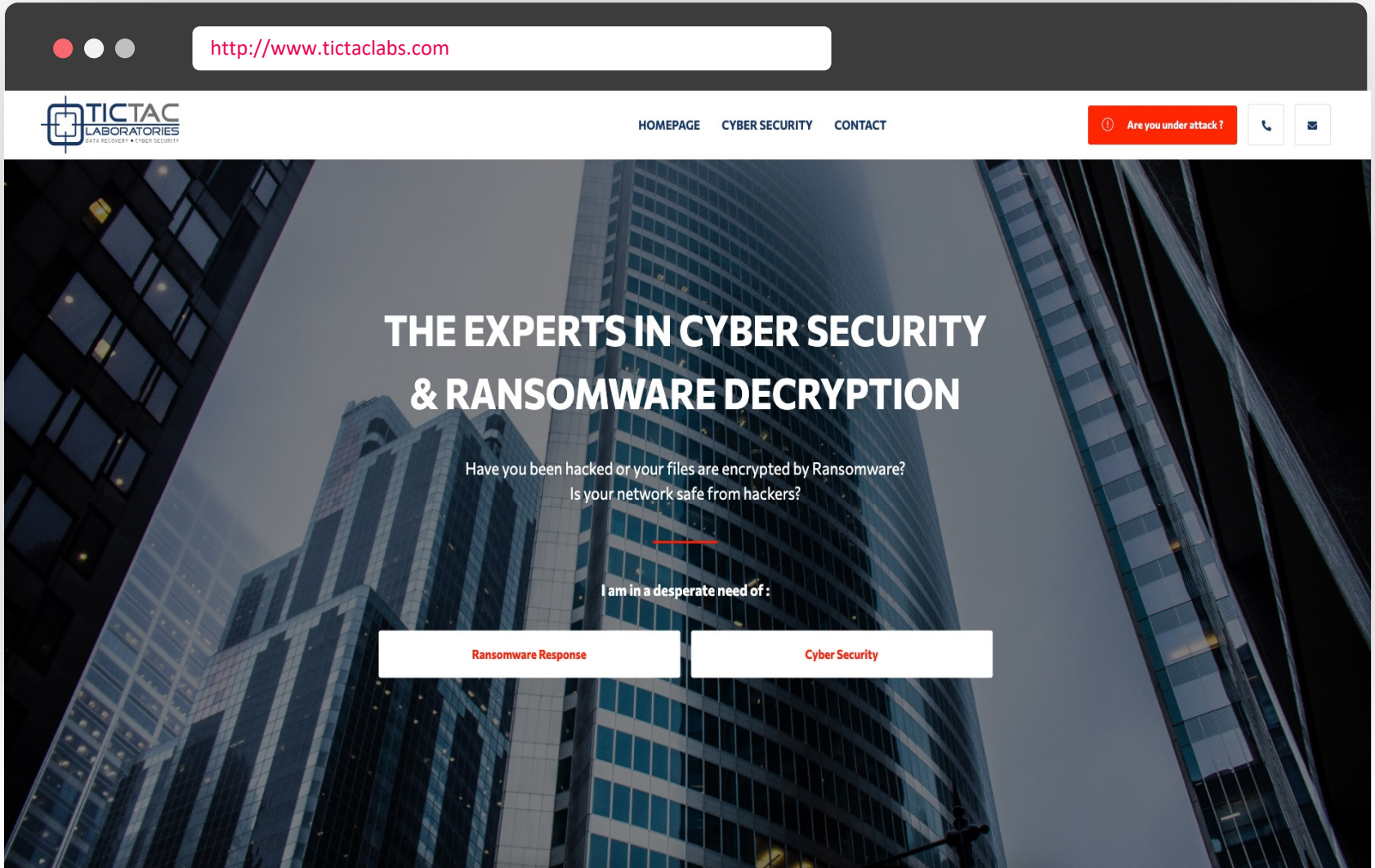
Επόμενο

Δωρεάν Τεστ Cyber Security: www.cybercheck.gr


English (Αγγλικά)
Ελληνικά
Home
Προσωπική και Οικογενειακή Προστασία
Προστασία Επιχειρήσεων
Επικοινωνία
Login
Buy Now
TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY
Digimune
Προστασία της Ψηφιακής Ταυτότητας & των Social Media
Προστατέψτε τον εαυτό σας, την οικογένεια σας και την επιχείρηση σας

Τριπόλεως 9, Υμηττός – Δάφνη
Τηλ. Κέντρο: 210 6897383
www.tictac.gr
www.tictaclabs.com

TICTAC CYBER SECURITY



Distributors for Greece & Cyprus for the following products:

COMODO CYBERSECURITY
SecurityScorecard
deepinstinct
Digimune powered by ZeroFOX
TARIAN

Resellers & Integrators for the following products:

Acronis | Platinum Partner
CyFIR
Microsoft Silver Partner
pfsense