Ransomware…
Ζουν ανάμεσά μας!

Στατιστικά χειρισμού πραγματικών υποθέσεων
και τρόποι προστασίας

Παναγιώτης Πιέρρος
GENERAL MANAGER
TicTac Data Recovery

Μιχάλης Μίγγος
TECHNICAL DIRECTOR
TicTac Data Recovery

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Ποιοί είμαστε και τι κάνουμε;

ΑΝΑΚΤΗΣΗ ΔΕΔΟΜΕΝΩΝ ΑΠΟ:

+ Χαλασμένους Σκληρούς δίσκους
+ Χαλασμένα USB Stick
+ Χαλασμένα Raid Συστήματα
+ Κινητά τηλέφωνα
+ Καταγραφικά Καμερών
+ Διεγραμμένα αρχεία
+ Βάσεις Δεδομένων
+ Κλειδωμένα Excel, Access αρχεία

Ποιοί είμαστε και τι κάνουμε;

Επίσης πριν συμβεί το κακό:

+ **Cyber Security** (Penetration Testing, Ransomware Incident Response)
+ **Disaster Recovery Plan** (Cloud Backup)
+ **Ασφαλής Καταστροφή Δεδομένων**
+ **Ηλεκτρονική Έρευνα** (Computer Forensics)
+ **Δικαστική Πραγματογνωμοσύνη** σε Υποθέσεις Ηλεκτρονικού Εγκλήματος

Το 2016 σας μιλήσαμε για το μέλλον

Το μέλλον των Ransomware είναι σήμερα… και έπεται και συνέχεια

Πλέον αποτελεί ολόκληρη βιομηχανία που αποδίδει για τους εγκληματίες

Τι είναι το Ransomware;

Είναι ένα είδος ιού υπολογιστών

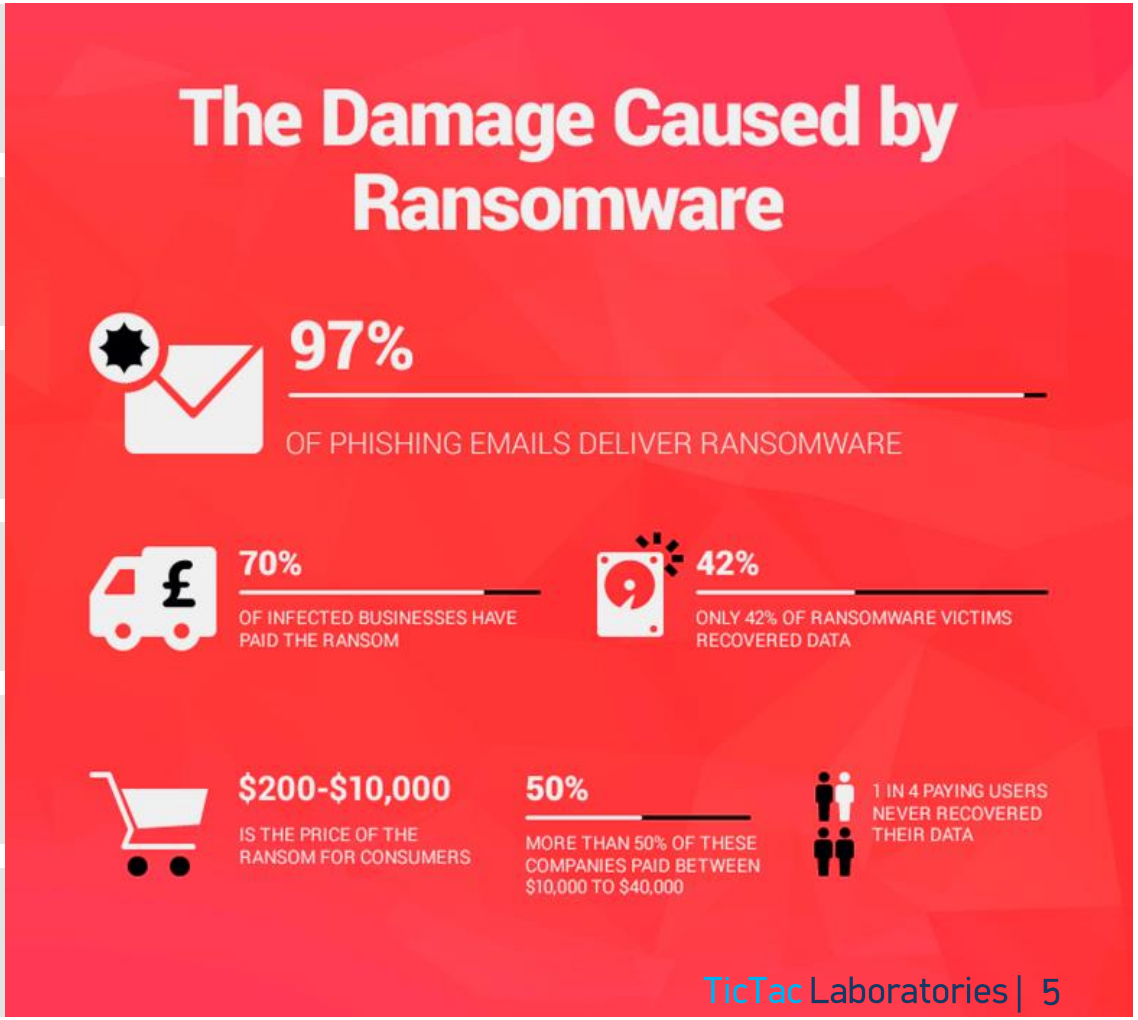
Αντί να σβήνει ή να καταστρέφει αρχεία, τα **κλειδώνει τα αρχεία** με τρόπο που μόνο ο κατασκευαστής του ιού μπορεί να δώσει λύση (συνήθως)

Ζητάει λύτρα (συνήθως 1000$ - 10.000$) για να πάρεις τα αρχεία σου, σε Bitcoin

Δεν τον εντοπίζουν συνήθως τα αντιβιοτικά/antivirus

Κλειδώνει και τα Backup!

Στις μέρες μας υπάρχουν **RaaS** (Ransomware as a Service)



Ransomware Marketplace Report

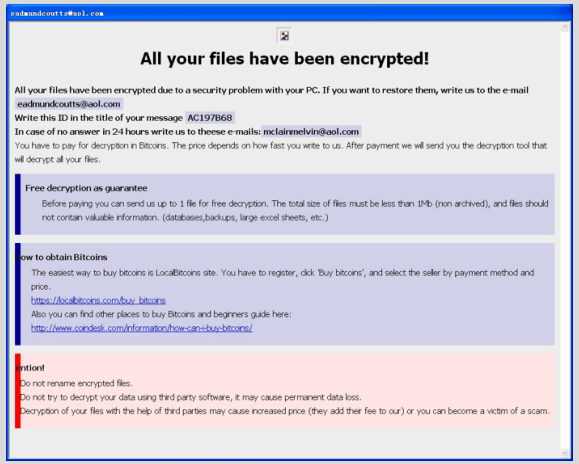
Ψηφιακά Λύτρα, Στατιστικά και Τρόποι Προστασίας

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Χαρακτηριστικά βασικών Τύπων Ransomware

Dharma (.cezar) - 63% των περιστατικών

Συνήθεις Στόχοι	Πολύ μικρές και μικρομεσαίες εταιρίες
Μέση Διάρκεια Περιστατικού	**5 ημέρες** (Πολύπλοκο εργαλείο αποκρυπτογράφησης, συχνά λάθη από μηχανογράφους, ελλείπεις οδηγίες από τους Hackers μετά την πληρωμή και κακή επικοινωνία)
Προβλήματα αποκρυπτογράφησης	Το εργαλείο αποκρυπτογράφησης δεν δουλεύει πάντα σωστά. Απαιτεί τεχνογνωσία. Γίνονται συχνά λάθη από τους μηχανογράφους που μπορεί να αποτρέψουν την αποκρυπτογράφηση ακόμα και αν πληρωθούν λύτρα.
Μέσο ποσό λύτρων	**5065$** ανά ID / περιστατικό

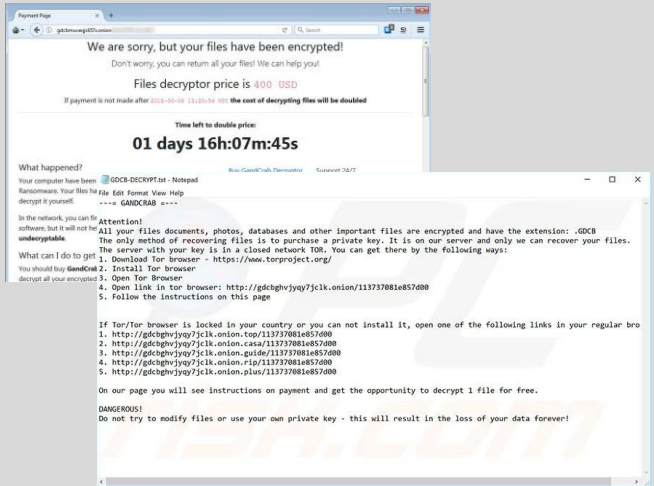


Κάποια Dharma File Extensions

.BIP .combo .gamma .arrow .betta .vanss .audit .adobe .fire .bear .back .cccmn .tron .like .gdb .myjob .risk .santa .bizer .btc .auf .heets .usa .qwx .xwx .aqva .eth .amber .stuf .ms13 .bk666 .com

Gandcrab - 16% των περιστατικών

Συνήθεις Στόχοι	Πολύ μικρές εταιρίες και ιδιώτες. Υπάρχει λύση χωρίς πληρωμή λύτρων υπό προϋποθέσεις.
Μέση Διάρκεια Περιστατικού	**3 ημέρες** (Προσφέρει αυτοματοποιημένες διαδικασίες όμως το εργαλείο αποκρυπτογράφησης είναι ιδιαίτερα αργό)
Προβλήματα αποκρυπτογράφησης	Λάθη πελατών / μηχανογράφων στον χειρισμό κρυπτονομισμάτων. Αργοπορία στο χειρισμό κοστίζει διπλασιασμό της τιμής των λύτρων. Στενά περιθώρια πληρωμής.
Μέσο ποσό λύτρων	**2721$** ανά ID / περιστατικό



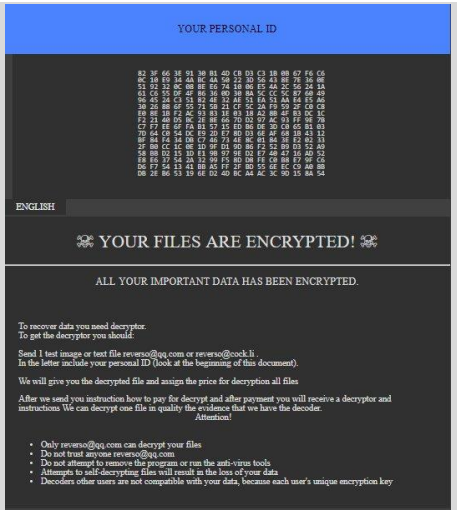
Κάποια Gandgrab File Extensions

.1st, .602, .7z, .7-zip, .abw, .act, .adoc, .aim, .ans, .apkg, .apt, .arj, .asc, .asc, .ascii, .ase, .aty, .awp, .awt, .aww, .cab, .doc, .docb, .docx, .dotm, .gzip, .iso, .lzh, .lzma, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .rar, .sldm, .sldx, .tar, .vbo, .vdi, .vmdk, .vmem, .vmx, .xla, .xlam, .xll, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xps, .z, .zip

Χαρακτηριστικά βασικών Τύπων Ransomware

Globeimposter - 6% των περιστατικών

Συνήθεις Στόχοι	Πολύ μικρές και μικρομεσαίες εταιρίες
Μέση Διάρκεια Περιστατικού	**6 ημέρες** (Πολύπλοκο εργαλείο αποκρυπτογράφησης, συχνά λάθη από μηχανογράφους, ελλείπεις οδηγίες από τους Hackers μετά την πληρωμή και κακή επικοινωνία)
Προβλήματα αποκρυπτογράφησης	Το εργαλείο αποκρυπτογράφησης δεν δουλεύει πάντα σωστά. Απαιτεί τεχνογνωσία. Γίνονται συχνά λάθη από τους μηχανογράφους που μπορεί να αποτρέψουν την αποκρυπτογράφηση ακόμα και αν πληρωθούν λύτρα.
Μέσο ποσό λύτρων	**4894$** ανά ID / περιστατικό



Κάποια Globeimposter File Extensions

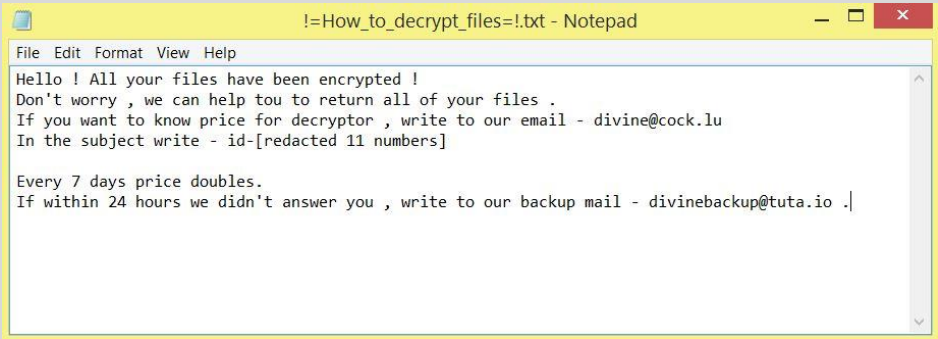
0.402, 0.4035, 0.409,0.4091, 0.452,.au1crypt,.BONUM,.BRT92,.BUSH,.C8B089F,.CHAK,.clinTON,.crypt,.FIX,.fuck,.goro,.gotham,.granny,.happ,.lpcrestore,.keepcalm,.LIN,.MAKB,.medal,.mtk118,.needdecrypt,.needkeys,.NIGGA,.nWcrypt,.paycyka,.pizdec,.pscrypt,.ReaGAN,.rumblegoodboy,.s1crypt,.scorp,.sea,.skunk,.Trump,.txt,.UNLIS,.vdul,.wallet,.write_on_email,.write_us_on_email,.YAYA,.zuzya,..doc,.encencenc,.lock,.Nutella,.waiting4keys,.FREEMAN,

Everbe 2.0 - 3% των περιστατικών

Συνήθεις Στόχοι	Πολύ μικρές εταιρίες και ιδιώτες.
Μέση Διάρκεια Περιστατικού	**5 ημέρες**
Προβλήματα αποκρυπτογράφησης	Λάθη πελατών / μηχανογράφων στον χειρισμό κρυπτονομισμάτων. Αργοπορία στο χειρισμό κοστίζει διπλασιασμό της τιμής των λύτρων. Στενά περιθώρια πληρωμής.
Μέσο ποσό λύτρων	**4321$** ανά ID / περιστατικό

Everbe 2.0 File Extensions

.evil

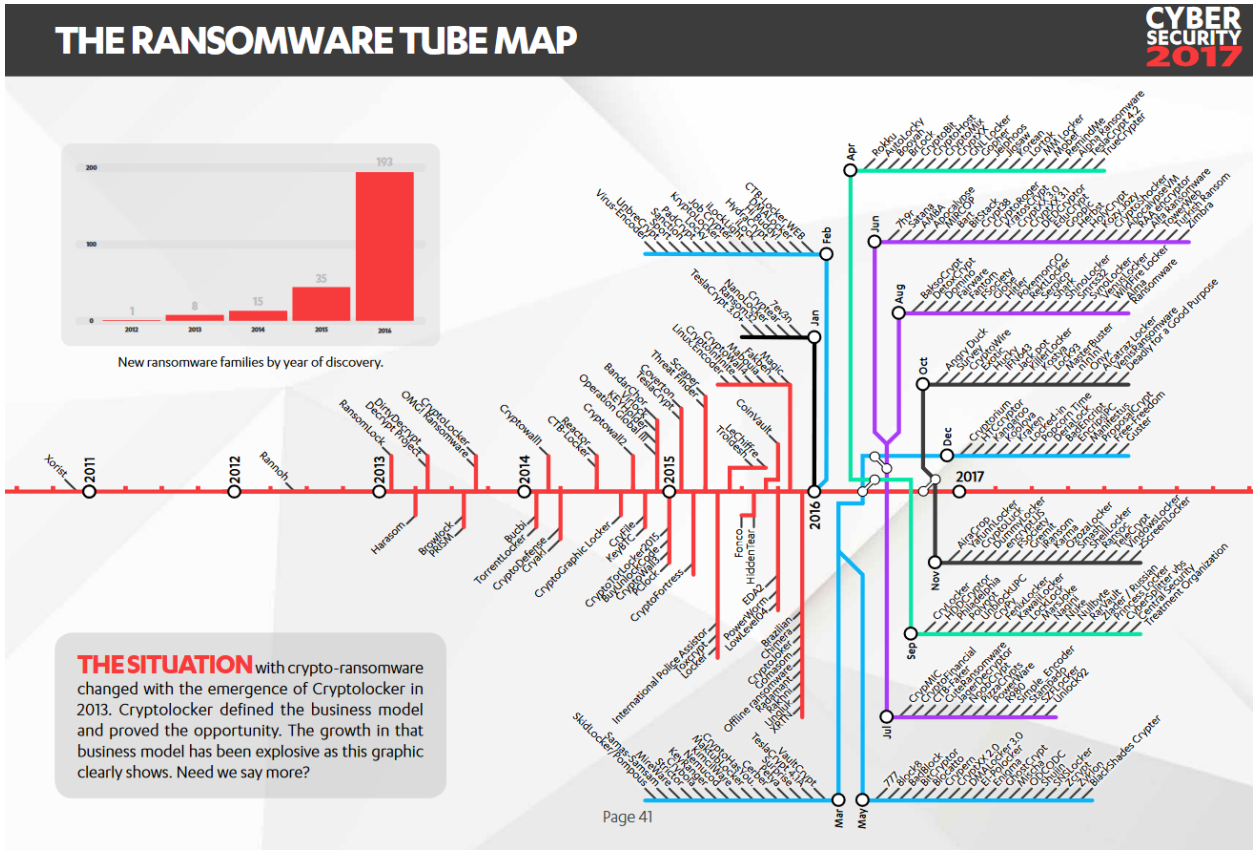


Υπάρχουν εκατοντάδες άλλα διαφορετικά είδη

- Wannacry
- Locky
- Notpetya
- Cerber
- Spora
- Rapid
- STOP (Djvu)
- ACCDFISA V2
- Mole
- THT Ransomare

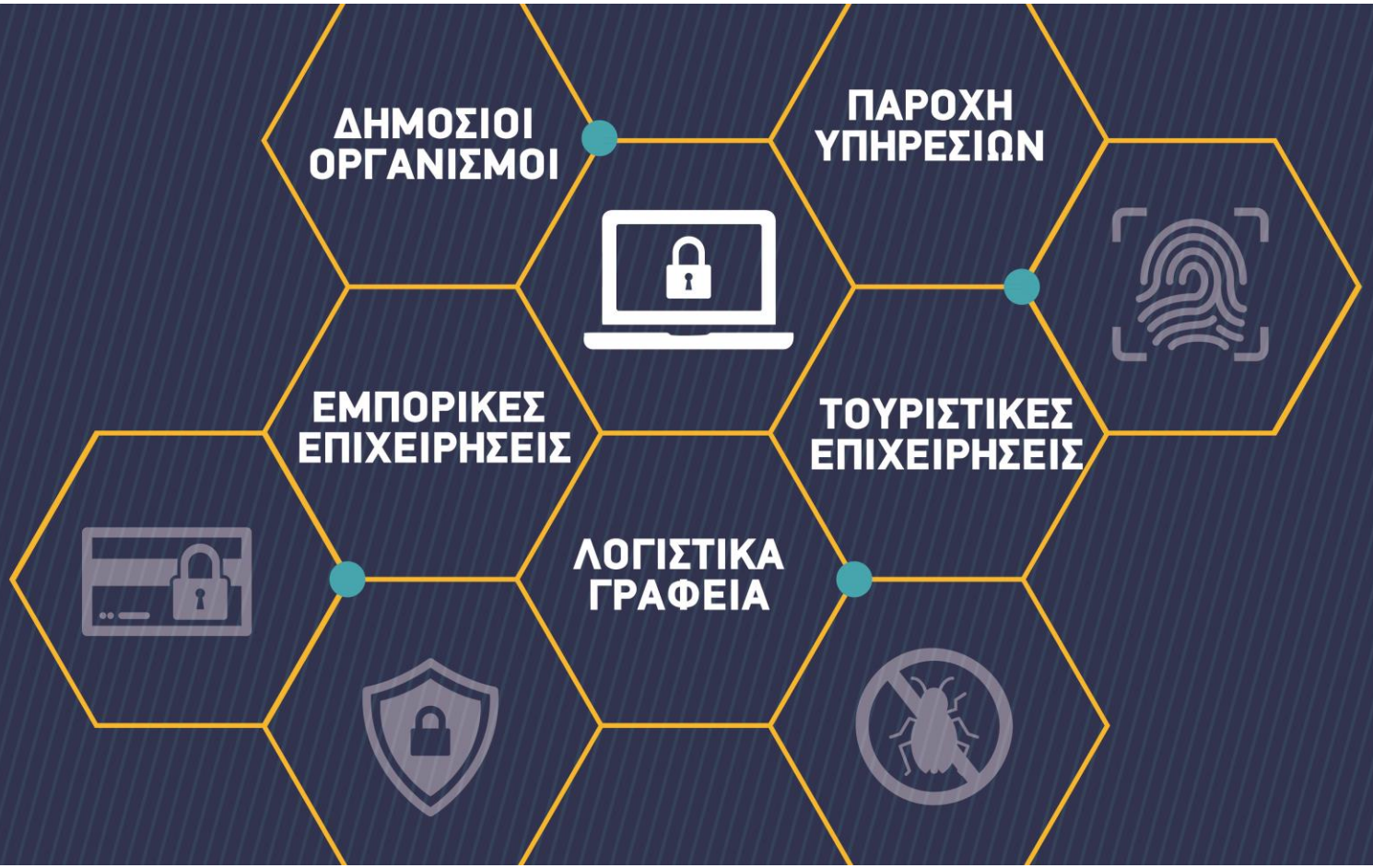
...και πολλά άλλα

Σε μόλις 6% των περιπτώσεων συνολικά μπορεί κανείς να αποκρυπτογραφησει χωρίς πληρωμή ή μπορούμε να ανακτήσουμε αρχεία μέσω διαδικασίας λογικής ανάκτησης δεδομένων



Πηγή:https://fsecurepressglobal.files.wordpress.com/2017/02/cyber-security-report-2017.pdf

Κλάδοι που έχουν χτυπηθεί περισσότερο

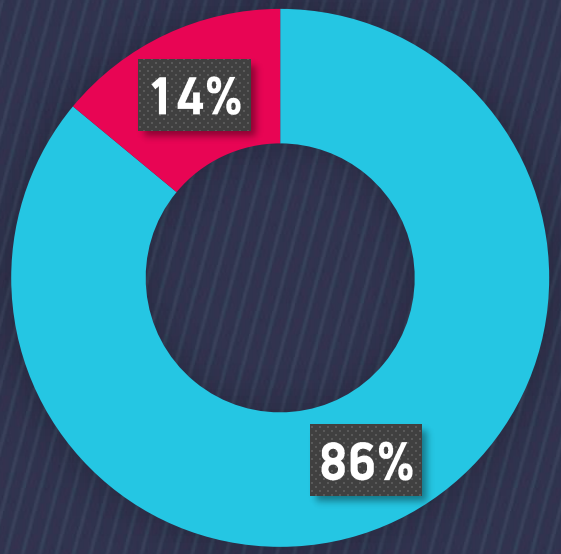


Μέσος όρος εργαζομένων

8

Κλάδοι που έχουν χτυπηθεί περισσότερο

Τεχνικό Τμήμα

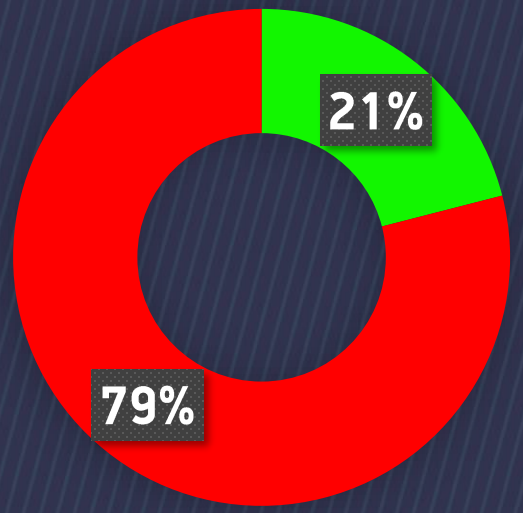


ΕΞΩΤΕΡΙΚΟ ΕΣΩΤΕΡΙΚΟ

Μέσος όρος Workstations / Servers

11

Το backup λειτούργησε;



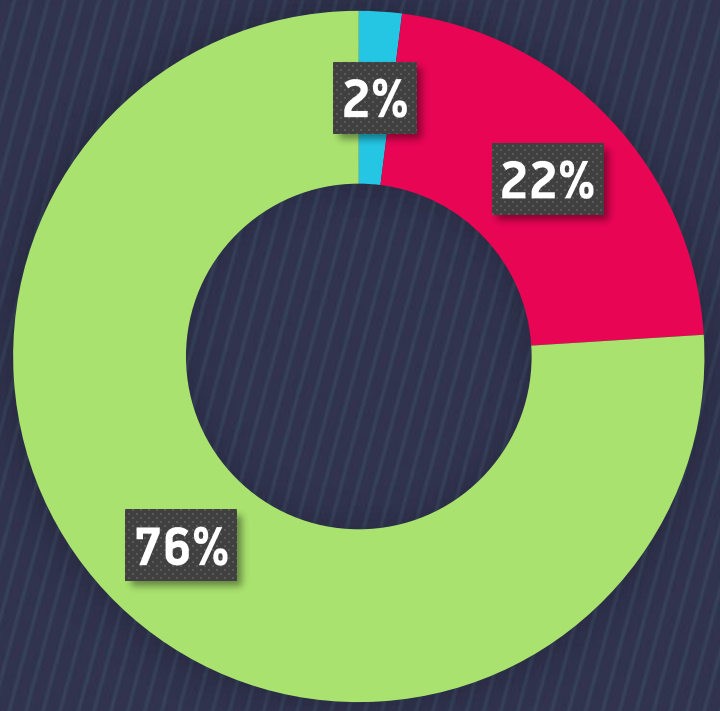
ΝΑΙ ΟΧΙ

Πραγματικά κόστη μιας επίθεσης Ransomware

Μέσος χρόνος διάρκειας περιστατικού	Μέσο κόστος Επαναφοράς Δεδομένων	Μέσο Κόστος Προσωρινής Διακοπής Εργασιών Εταιρίας
5.7 μέρες	8.284 ευρώ	23.452 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

Πώς εισέρχονται Ransomware στην υποδομή μας;



- SOCIAL ENGINEERING
- PHISHING / EMAIL ATTACHMENTS
- RDP

Η βασική πηγή εισόδου είναι πάντα τα **Compromised RDP**

Τον τελευταίο καιρό διαπιστώσαμε , από περιστατικά στα οποία έγινε Digital Forensics Analysis & Penetration Testing, πως οι επιτιθέμενοι βρίσκονται στην υποδομή αρκετό χρονικό διάστημα, μελετώντας τους πόρους και εντοπίζοντας και τις υποδομές Backup, ώστε να τις κρυπτογραφήσουν για να έχουν μέγιστο αποτέλεσμα στον εκβιασμό.

Για τις εταιρίες IT Support που έχουν πελάτες με Remote Support παρατηρήθηκε στο εξωτερικό ότι οι επιτιθέμενοι υποκλέπτουν τα στοιχεία πρόσβασης των πελατών τους και επιτίθενται μαζικά και σε αυτούς.

Δεν είμαστε υπέρ της πληρωμής λύτρων

Οι αρχές συμβουλεύουν να μην πληρωθούν τα λύτρα

Από το εργαστήριο μας γίνεται **κάθε δυνατή προσπάθεια για να βρεθεί λύση** χωρίς πληρωμή λύτρων

Σκοπός μας όμως είναι ο πελάτης να πάρει πίσω τα αρχεία του, με όποιο τρόπο είναι διαθέσιμος

Παρόλο που **η TicTac τάσσεται εναντίον της πληρωμής των λύτρων**, καθώς παίζουμε το παιχνίδι του εκβιαστή, μερικές φορές **δεν υπάρχει άλλη λύση από την πληρωμή των λύτρων**. Σε τέτοιες **περιπτώσεις μπορούμε να βοηθήσουμε άμεσα, αλλά υπό προϋποθέσεις.**

Τι μπορεί να πάει στραβά αν πληρώσετε;

Να χάσουμε την τρέχουσα κρυπτογραφημένη κατάσταση και να μην είναι δυνατή η επαναφορά ακόμα και με πληρωμή!

- Από λάθος του μηχανογράφου
- Από αστοχία δίσκου
- Από διπλή κρυπτογράφηση από άλλο Hacker
- Από λάθος εκτέλεση του Decryptor

Να έχουμε πέσει σε ομάδα κακοποιών που **θα πάρουν τα χρήματα και θα εξαφανιστούν**

Να μην γνωρίζει ο εγκληματίας πως γίνεται η αποκρυπτογράφηση

Τι μπορεί να πάει στραβά αν πληρώσετε;

- Να μην δώσουν οι Hacker σωστές οδηγίες και να γίνουν τα πράγματα χειρότερα από πριν
- Να εκβιάσουν για περισσότερα λύτρα μετά την πρώτη πληρωμή
- Να γίνει λάθος στην πληρωμή κρυπτονομισμάτων (WORKSHOP)
- Να πέσουμε θύμα απάτης στην αγορά κρυπτονομισμάτων
- Να αργήσουμε και ο Hacker να εξαφανιστεί ή να αυξήσει την τιμή

Ransomware Incident Response by Tictac
Εχουμε Σύστημα που φέρνει αποτέλεσμα!

01 Ο Ρόλος του διαπραγματευτή/συντονιστή είναι να κάνει αξιολόγηση της απώλειας

02 Παίρνουμε δείγμα και γίνονται οι απαραίτητοι έλεγχοι
να δούμε αν υπάρχει διαθέσιμη λύση στο εργαστήριο
μας ή ελεύθερη στο Internet

03 Ελέγχουμε την αξιοπιστία του εγκλήματία στο Dark Web και από τη
Βάση δεδομένων μας

04 Καθοδηγούμε στην αγορά Bitcoin ή Βοηθάμε στην εύρεση των Bitcoin
(κρυπτονομισμάτων) με αξιόπιστους πωλητές άμεσα

05 Εκπαιδεύουμε και καθοδηγούμε τον πελάτη, ούτως ώστε αν θέλει να
πληρώσει τα λύτρα, να το κάνει σωστά

06 Βοηθάμε στη διαπραγμάτευση με τον Hacker (όταν βλέπουμε ότι είναι εφικτό)

07 Είμαστε στο πλευρό του μηχανογράφου της επιχείρησης (με Remote Support)

CYBER DEFENSE LABS

Το Σύστημα της ομάδας Ransomware Incident Response της Tictac, <u>φέρνει το βέλτιστο δυνατό αποτέλεσμα με το ελάχιστο Downtime</u>

Προστασία από Ransomware και επιθέσεις

Τα κλασσικά μέσα δεν βοηθούν στην προστασία σας!

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Προτάσεις προστασίας για το 2019

01. Cloud Backup:

Αυτοματοποιημένη λύση Backup σε τοπικό χώρο αποθήκευσης και στο Cloud

- Δοκιμασμένη προστασία από Ransomware
- Κρατάει τις διάφορες εκδόσεις των αρχείων
- Προστατεύει από Διαγραφές

Κάντε κλικ εδώ για να δείτε πληροφορίες στο Site μας

Προτάσεις προστασίας για το 2019

02. Penetration Test / Vulnerability Test:

Δοκιμές των τεχνολογικών υποδομών σας για επιθέσεις Hacker.

Η Cyber Security Team της Tictac προσπαθεί να «εισέλθει» στις υποδομές σας, πριν εισέλθει κάποιος τρίτος!

Κάντε κλικ εδώ για να δείτε πληροφορίες στο Site μας

Προτάσεις προστασίας για το 2019

03. WEB Content Filtering:

Φιλτράρετε το περιεχόμενο του δικτύου σας, ελέγξτε με Reports τι είναι επικίνδυνο και θέστε τα δικά σας φίλτρα σε όλο το δίκτυο σας (π.χ. φραγή Social Media ή Αθλητικών Site κλπ)

Προτάσεις προστασίας για το 2019

04. Εκπαίδευση Προσωπικού για ασφαλή διαχείριση δεδομένων & πλοήγηση στο Internet:

- Αποτροπή Phishing
- Αποτροπή Social Engineering επιθέσεων
- Αναγνώριση Malware

Προτάσεις προστασίας για το 2019

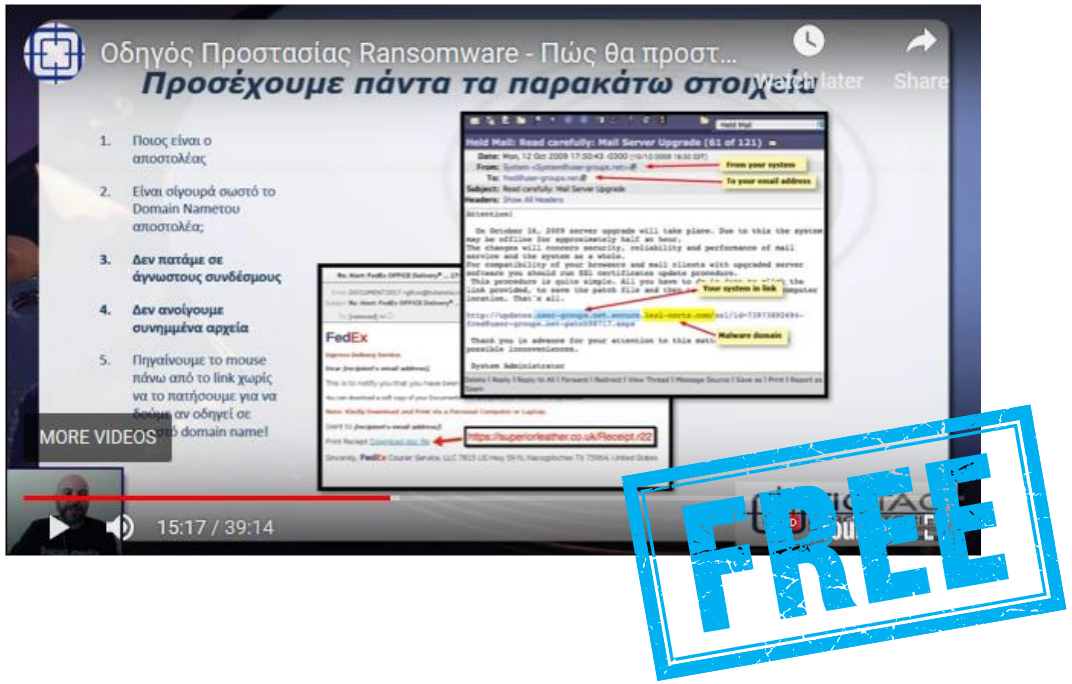
05. Ασφάλεια Cyber Insurance

Προστασία από τις οικονομικές επιπτώσεις μιας επίθεσης Hacker/Ransomware

- Καλύπτει τα κόστη αποκατάστασης του IT
- Επίσης καλύπτει νομικές κυρώσεις και ότι άλλο προκύψει

TICTAC LABORATORIES
DATA RECOVERY • CYBER SECURITY

Κατεβάστε τον
Οδηγό προστασίας Ransomware



http://tictac.gr/go/ransomware-protection

Κάντε εγγραφή στο Newsletter της Tictac