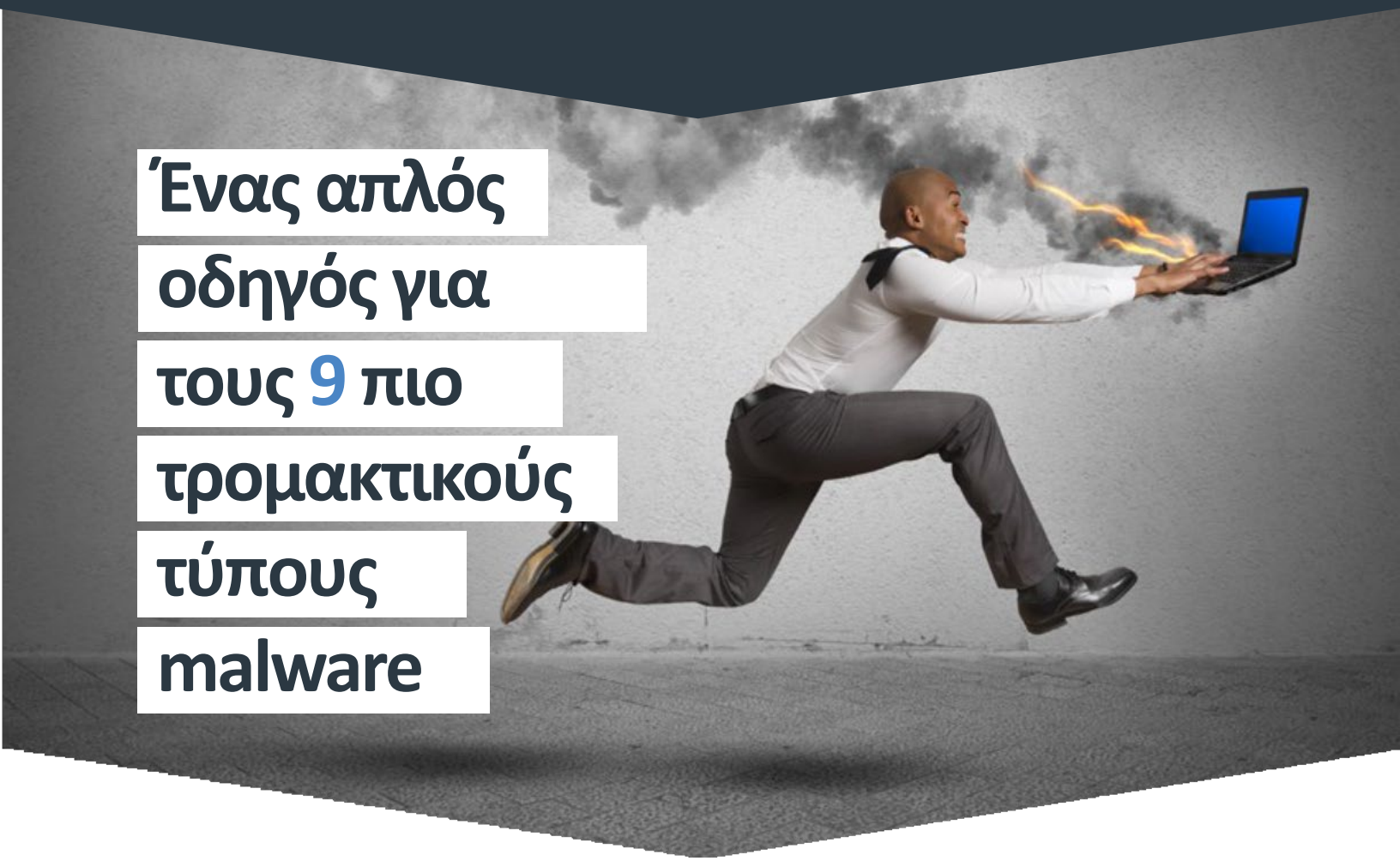
Αυτές είναι οι απειλές που πρέπει να σας ανησυχούν



Ένας απλός οδηγός για τους 9 πιο τρομακτικούς τύπους malware

GIANT STRIDE
IT SUPPORT

Ήταν πολύ πιο απλό

Όσο μεγαλώναμε...

Εάν είχατε δανειστεί ποτέ μια δισκέτα από έναν φίλο και τη βάζατε στον υπολογιστή σας, διατρέχατε τον κίνδυνο να κολλήσετε ιό (στον υπολογιστή σας).

Η απάντηση σε αυτό ήταν απλή: Οι περισσότεροι εγκαθιστούσαν ένα antivirus - και αυτό ήταν!

Όμως ήρθαν δύο μεγάλα πράγματα που άλλαξαν τα πάντα: το internet και η απληστία.

Βλέπετε, τότε, οι περισσότεροι ιοί υπολογιστών γράφτηκαν για διασκέδαση και για να κάνουν επίδειξη των δεξιοτήτων τους οι Χάκερς. Προσπαθούσαν να εισέλθουν σε υπολογιστές και να αποκτήσουν πρόσβαση σε πληροφορίες για την αναγνώριση και όχι για την οικονομική επιβράβευση.

Στις μέρες μας το hacking είναι επάγγελμα. Και πολύ επικερδές μάλιστα. Το internet έχει κάνει πολύ εύκολη τη πρόσβαση σε γνώσεις hacking, καθώς και σε ισχυρά αυτοματοποιημένα εργαλεία.

Υπάρχει και το οργανωμένο έγκλημα που εμπλέκεται στο σύγχρονο hacking. Οι εγκληματίες είναι συστηματικοί, διεξοδικοί και αδίστακτοι με τις επιθέσεις τους.

Πιστέψτε μας όταν σας λέμε ότι όλες οι επιχειρήσεις αποτελούν στόχο για τους Χάκερς διαρκώς. Τα αυτοματοποιημένα εργαλεία το κάνουν εύκολο.

Μην αφήνετε ποτέ κανέναν να σας ξεγελάσει με μια ψευδή αίσθηση ευεξίας σχετικά με ζητήματα ασφάλειας στο IT.

Βλέπουμε κυβερνοεπιθέσεις σε επιχειρήσεις σχεδόν καθημερινά. Κυρίως βλέπουμε στοιχεία αποτυχημένων επιθέσεων καθώς οι επιχειρήσεις που έχουμε αναλάβει είναι καλά προετοιμασμένες και προστατευμένες.

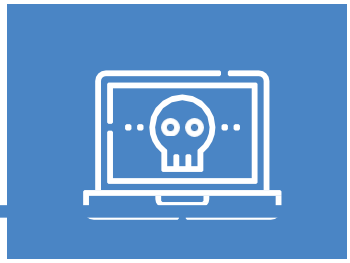
Ωστόσο, περιστασιακά μιλάμε με επιχειρηματίες και διευθυντές, με τους οποίους ακόμα δεν συνεργαζόμαστε και έχουν πληγεί. Οι συνέπειες μπορεί να είναι καταστροφικές ανάλογα με το τι τους συνέβη.

Οτιδήποτε έχει σχεδιαστεί για να υποκλέψει τα δεδομένα σας ή να βλάψει τα συστήματα και τους υπολογιστές σας ονομάζεται κακόβουλο λογισμικό "malicious software".

Υπάρχουν διάφοροι τρόποι με τους οποίους μπορείτε να γίνετε στόχος. Το να έχετε επίγνωση της κατάστασης είναι η πρώτη σας άμυνα.

Αυτός είναι ο οδηγός μας για τα 9 πιο τρομακτικά είδη κακόβουλου λογισμικού.

1. Ιοί



Το κακόβουλο λογισμικό είναι πλέον πολλά περισσότερα από ένας απλός ιός. Για αυτό χρειάζεστε μεγαλύτερη άμυνα από ένα antivirus.

Οι ιοί επιτίθονται μολύνοντας, διαγράφοντάς ή μορφοποιώντας τα αρχεία σας, κάνοντας πολύ δύσκολο τον καθαρισμό τους. Συχνά, οι ιοί λειτουργούν αντιγράφοντας τον εαυτό τους, ή πλημμυρίζοντας δίκτυα υπολογιστών, καθιστώντας αδύνατη την εκτέλεση ακόμα και απλών εργασιών.

Ο καθαρισμός των αρχείων και του υπολογιστή σας μπορεί να είναι από δύσκολος έως σχεδόν αδύνατος. Συχνά, για να λειτουργήσουν ξανά όλα - θα πρέπει να διαγράψετε τα αρχεία που έχουν επηρεαστεί. Πιθανώς να χρειαστεί να ξαναστήσετε τους υπολογιστές σας από το μηδέν.

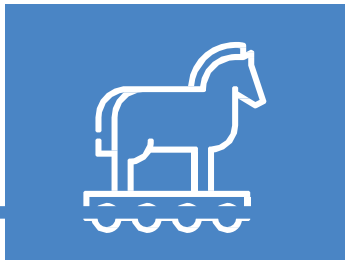
2. Worms

Τα Worms υπάρχουν από τη δεκαετία του 90. Αρκεί ένα μολυσμένο email... για να εξαπλωθούν στη συνέχεια σε όλο το εταιρικό δίκτυο.

Το τρομακτικό με τα Worms είναι ότι σε αντίθεση με έναν ιό, δεν χρειάζεται να προβείτε σε καμία ενέργεια για να τα διαδώσετε. Τα Worms αναπαράγονται και εκμεταλλεύονται άλλο λογισμικό για να κάνουν τη δουλειά τους.

Μπορεί να έχετε ακούσει για το Worm "Iloveyou", το οποίο βγήκε πριν από 21 χρόνια. Επηρέασε 50 εκατομμύρια υπολογιστές Windows σε όλο τον κόσμο σε μόλις 10 ημέρες. Αυτός είναι ο τρόπος που μπορούν να γίνουν ισχυρά και ασταμάτητα τα Worms.

3. Trojans



Τα Trojans έχουν σχεδόν αντικαταστήσει τα Worms – καθώς αποτελούν δημοφιλέστατα hacking εργαλεία. Είναι το νέο όπλο επιλογής.

Αυτός ο τύπος κακόβουλου λογισμικού εκμεταλλεύεται την έλλειψη γνώσεων ασφαλείας του εκάστοτε θύματος. Συνήθως, φτάνει σε εσάς με τη μορφή συνημμένου στο Email σας. Αυτά, αρχίζουν να μοιάζουν όλο και πιο αυθεντικά, οπότε είναι εύκολο να την πατήσετε και να τα ανοίξετε.

Μόλις ανοίξετε το συνημμένο .. μπαμ... τελειώσατε!

Τα Trojans μπορούν να εγκατασταθούν και αν επισκεφτείτε, απλά, ένα μολυσμένο website.

Δύσκολα ανιχνεύονται, καθώς δημιουργούνται πανεύκολα και εγκαθίστανται από τα ίδια τα θύματα που τα ανοίγουν κατά λάθος.

4. Hybrids

Μπορεί να έχετε συσχετίσει τα hybrids με «πράσινα» αυτοκίνητα. Ωστόσο, δεν υπάρχει τίποτα καλό σε ένα υβριδικό κακόβουλο λογισμικό.

Ρίξτε μια ματιά στα 3 πρώτα είδη κακόβουλου λογισμικού για τα οποία μιλήσαμε και πόσο δύσκολο είναι να αντιμετωπιστούν.

Ένα υβρίδιο είναι κακόβουλο λογισμικό με διαφορετικά χαρακτηριστικά, όπως η μεταμφίεση ενός trojan και η δύναμη ενός worm.

Όπως μπορείτε να φανταστείτε, με τα υβρίδια μπορεί να είναι πολύ δύσκολος ο καθαρισμός μετά από μια επίθεση.

5. Ransomware

Αυτό μπορεί να είναι 5ο στη λίστα μας, αλλά το ransomware είναι το κακόβουλο λογισμικό που φοβούνται περισσότερο οι επαγγελματίες πληροφορικής.

Το Ransomware είναι ίσως ότι χειρότερο αυτήν τη στιγμή. Και επιχειρήσεις σαν τη δική σας είναι ο πρωταρχικός στόχος.

Λειτουργεί κρυπτογραφώντας όλα σας τα δεδομένα για να σας κρατάει «όμηρους». Κυριολεκτικά δεν έχετε καθόλου δεδομένα - κανένα αρχείο πελατών, αρχεία office, μηνύματα ηλεκτρονικού ταχυδρομείου, τίποτα. Μπορείτε να φανταστείτε πόσο τρομακτικό είναι αυτό;

Οι χάκερς απαιτούν να πληρώσετε λύτρα για να ελευθερώσουν τα δεδομένα σας και να τα επιστρέψουν σε εσάς. Αυτό μπορεί να σας κοστίσει χιλιάδες ευρώ, και ζητούν την αμοιβή σε Bitcoin που είναι ιδιαίτερα δύσκολο να εντοπιστούν.

Τα περισσότερα ransomware είναι trojan, που σημαίνει ότι βασίζονται σε εσάς που θα τα ενεργοποιήσετε κατά λάθος ανοίγοντας ένα συνημμένο ή μια ιστοσελίδα.

Δυστυχώς, αυτό το είδος επίθεσης είναι πολύ δύσκολο να αντιμετωπιστεί - ο οικονομικός αντίκτυπος μπορεί να είναι τεράστιος - και αυτό χωρίς καν να πληρώσετε τα λύτρα.

Βεβαιωθείτε ότι κρατάτε (cloud) backups τακτικά για να αποφύγετε την ολοκληρωτική καταστροφή. Επίσης, πρέπει να εκπαιδεύεστε για να εντοπίζετε τα συμπτώματα μιας επικείμενης επίθεσης.

6. Fileless malware

Τεχνικά, δεν είναι διαφορετική κατηγορία, αλλά τη συμπεριλάβαμε γιατί αποτελεί πραγματική απειλή.

Περίπου οι μισές από τις επιθέσεις κακόβουλου λογισμικού προέρχονται από fileless malware - και αυτό αυξάνεται συνεχώς.

Ενώ το «παραδοσιακό» κακόβουλο λογισμικό βασίζεται στα αρχεία για τη μόλυνση, αυτή η μορφή βασίζεται στη μνήμη RAM και σε άλλες λειτουργίες του λειτουργικού σας συστήματος.

Αυτός ο τύπος επίθεσης είναι πολύ πιο δύσκολο να εντοπιστεί και να σταματήσει. Τα παραδοσιακά antivirus προγράμματα συχνά αδυνατούν να τα εντοπίσουν.

7. Adware

Βρίσκεστε σε έναν ιστότοπο. Υπάρχει ένα pop up. Κάνετε κλικ, και πριν το καταλάβετε, κάποιο λογισμικό έχει εγκατασταθεί στον υπολογιστή σας. Ή υπάρχει μια νέα προσθήκη στο πρόγραμμα περιήγησής σας, ή ξαφνικά χρησιμοποιεί άλλη μηχανή αναζήτησης.

Το Adware είναι ενοχλητικό παρά επικίνδυνο. Αλλά μπορεί να επιβραδύνει τους υπολογιστές, ή να τους κάνει ευάλωτους σε άλλες επιθέσεις.

Οτιδήποτε έχει εγκατασταθεί χωρίς τη ρητή σας άδεια είναι παράσιτο και πρέπει να αντιμετωπιστεί.

8. Malvertising

Δεν λατρεύετε ένα καλό μείγμα λέξεων;

Όπως ίσως μαντέψατε, το malvertising είναι κακόβουλο λογισμικό που κρύβεται πίσω από διαφημίσεις.

Μην το συγχέετε με adware. Η κακόβουλη διαφήμιση εμφανίζεται όταν ένας εγκληματίας στο κυβερνοχώρο *πληρώνει* για μια διαφήμιση σε έναν *πραγματικό ιστότοπο*.

Όταν κάνετε κλικ στη διαφήμιση, είτε ανακατευθύνεστε σε ένα κακόβουλο ιστότοπο είτε εγκαθίσταται κακόβουλο λογισμικό στη συσκευή σας.

Ακόμα και γνήσιες διαφημίσεις διακυβεύονται.

Το πιο τρομακτικό είναι ότι μερικές φορές δεν χρειάζεται καν να κάνετε κλικ στη διαφήμιση - αυτό ονομάζεται: drive-by.

9. Spyware

Ξανά, ένα πολύ περιγραφικό όνομα. Το spyware χρησιμοποιείται για να σας κατασκοπεύει.

Όταν εγκατασταθεί, το spyware μπορεί να παρακολουθεί τους ιστότοπους που επισκέπτεστε, όλα όσα πληκτρολογείτε (αυτό είναι γνωστό ως keylogging) και οποιεσδήποτε άλλες πληροφορίες σχετικά με εσάς και το τι κάνετε στη συσκευή σας.

Είναι ένας καλός τρόπος για να βρει κάποιος τα στοιχεία σύνδεσης και τους κωδικούς πρόσβασής σας.

Το λογισμικό υποκλοπής spyware ενεργοποιείται όταν κάνετε κλικ σε κάτι που δεν πρέπει, όπως συνημμένο αρχείο, pop up, κάποια ειδοποίηση.

Όπως το adware: το spyware είναι πιο εύκολο να το αφαιρέσετε, αλλά μέχρι να το βρείτε, πιθανότατα να έχετε δώσετε πολλές πολύτιμες πληροφορίες.

Ορίστε: Οι 9 πιο τρομακτικοί τύποι κακόβουλου λογισμικού και πώς θα επηρεάσουν εσάς και την επιχείρησή σας.

Ο αντίκτυπος που μπορεί να έχουν αυτές οι μορφές κακόβουλου λογισμικού κυμαίνεται από χαμένη παραγωγικότητα έως τη πλήρη πτώχευση.

Αυτός ο οδηγός αποτελεί μια απλή περίληψη. Δεν θέλουμε να σας τρομοκρατήσουμε με γεγονότα και αριθμούς. Ωστόσο, είναι ασφαλές να υποθέσετε ότι δεν θέλετε να αντιμετωπίσετε μια μεγάλη επίθεση στην επιχείρησή σας.

Θυμηθείτε τι είπαμε στην αρχή αυτού του οδηγού: Όλες οι επιχειρήσεις βάλλονται από Χάκερς διαρκώς.

Βεβαιωθείτε πως κάνετε ό,τι μπορείτε για να διατηρήσετε την επιχείρησή σας ασφαλή. Αυτό ξεκινά με τη δημιουργία μιας κουλτούρας για τη σοβαρή λήψη της ασφάλειας στο κυβερνοχώρο.

Συμβουλευτείτε έναν αξιόπιστο συνεργάτη IT για να βρείτε τον καλύτερο συνδυασμό λογισμικού, εκπαίδευσης και διαδικασιών.

Υπάρχουν πολλά που μπορούν να γίνουν για την προστασία της επιχείρησής σας - αλλά φυσικά πρέπει να γίνουν πριν συμβεί κάτι κακό.

Είμαστε εδώ για να σας διευκολύνουμε να αναλάβετε δράση. Το μεγαλύτερο μέρος της σκληρής δουλειάς μπορούμε να το κάνουμε εμείς για εσάς.

Καλέστε μας στο 211 198 5162 για να σας καθοδηγήσουμε