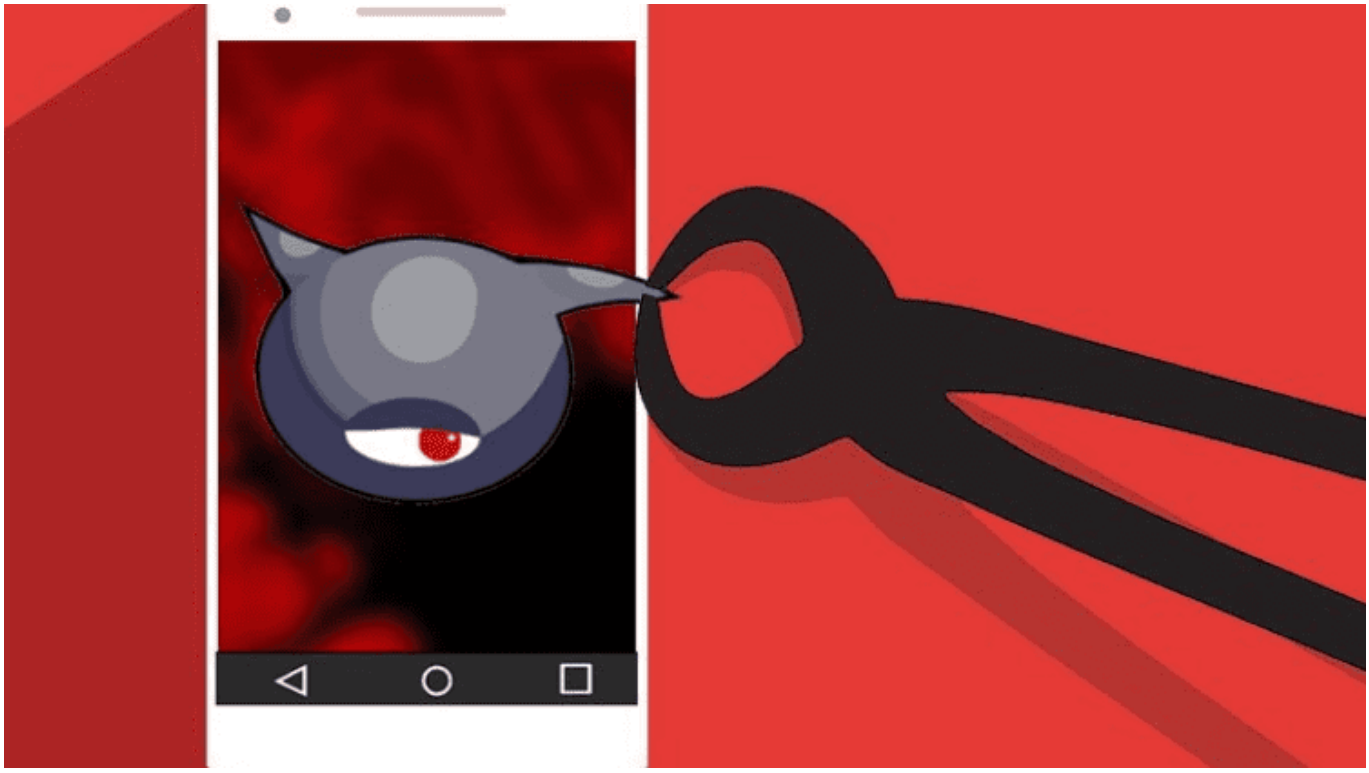
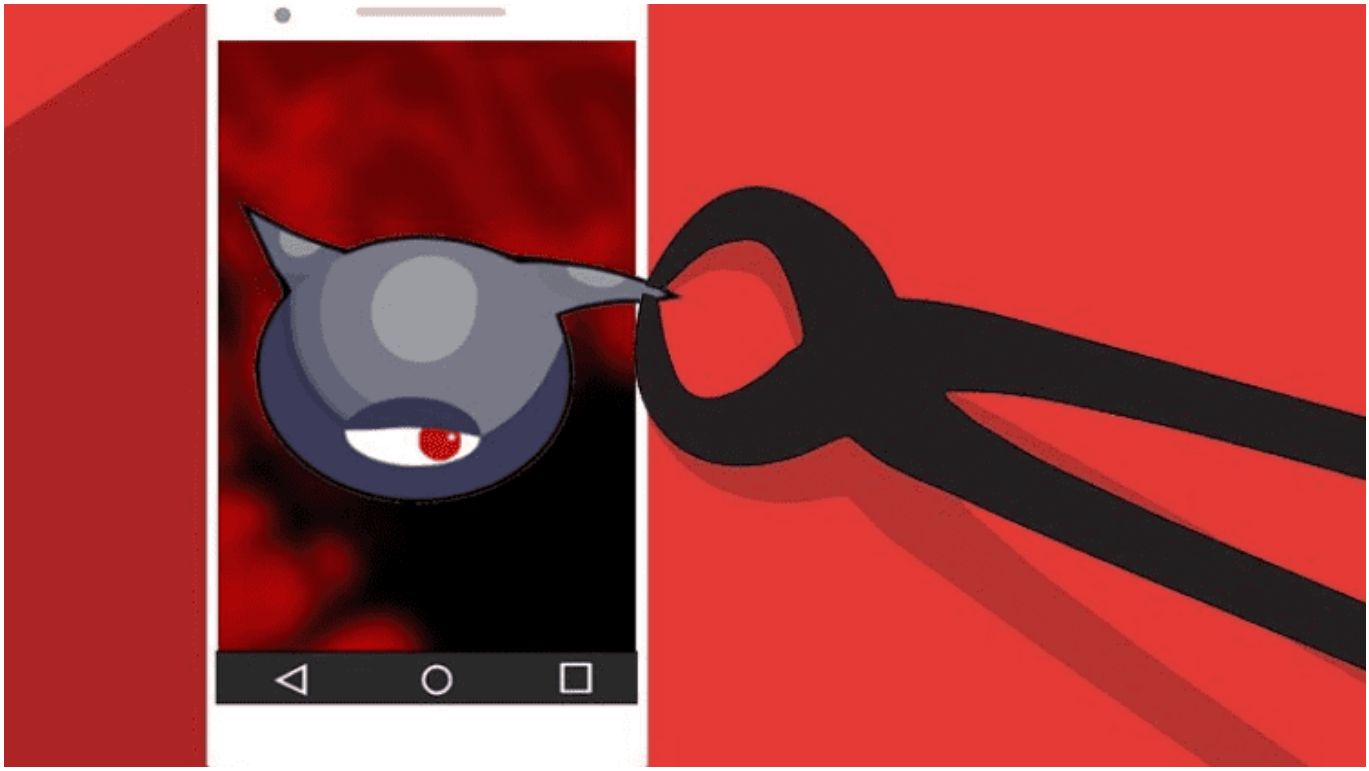
7 Ιανουαρίου 2020

Αφαίρεση ιών από κινητό χωρίς εργοστασιακή επαναφορά

/ Επιστήμες, Τέχνες & Πολιτισμός



Η εύκολη λύση για την αφαίρεση ιών από κινητό είναι η επαναφορά των εργοστασιακών ρυθμίσεων (factory reset). Όμως αυτό θα διαγράψει όλες μας τις εφαρμογές, και όλα μας τα προσωπικά αρχεία στο κινητό, μαζί και αναντικατάστατες φωτογραφίες και βίντεο. Δείτε όλα τα σημάδια που μας λένε ότι η συσκευή μας βρίσκεται σε κίνδυνο και πώς μπορεί να γίνει η αφαίρεση ιού από κινητό Android χωρίς εργοστασιακή επαναφορά.



Πώς διαφέρουν οι ιοί στο κινητό Android από τους ιούς στα Windows
Ως ιός στο Android θεωρείται το κακόβουλο λογισμικό που έχει τη δυνατότητα να προκαλεί δυσλειτουργίες στην συσκευή. Από το να εμφανίζει ανεπιθύμητες επιπλέον διαφημίσεις, μέχρι να υποκλέπτει όλα τα ευαίσθητα προσωπικά μας δεδομένα.

Ο ίδιος βασικός ορισμός αφορά και το αντίστοιχο κακόβουλο λογισμικό στα Windows. Όμως η βασική διαφορά είναι στο πώς μπορεί να κολλήσει μια μόλυνση ένας υπολογιστής σε σχέση με ένα κινητό.

Τόσο το ίδιο το λειτουργικό σύστημα, όσο και ο τρόπος που το χρησιμοποιούμε, κάνουν το Android σημαντικά πιο ασφαλές από κακόβουλες μολύνσεις σε σχέση με τα Windows.

Αυτό όμως δεν σημαίνει πως το κινητό Android είναι απρόβλητο από ιούς. Και τον μεγαλύτερο κίνδυνο διατρέχουν όσοι εγκαθιστούν εφαρμογές εκτός Play Store, μέσω αρχείων apk από άγνωστες και ύποπτες πηγές.

Ο κίνδυνος πολλαπλασιάζεται όταν αυτά τα apk αφορούν σπασμένες εφαρμογές και παιχνίδια, για να έχουμε δωρεάν κάποια χαρακτηριστικά που κανονικά είναι διαθέσιμα επί πληρωμή.

Όσοι ακολουθούν αυτή την πρακτική, αργά ή γρήγορα κάτι θα κολλήσουν και θα χρειαστεί να προχωρήσουν σε αφαίρεση ιού από κινητό. Είναι απλά θέμα χρόνου.

Ωστόσο, αυτό δεν σημαίνει πως όσοι εγκαθιστούν εφαρμογές αποκλειστικά από το Google Play είναι απόλυτα ασφαλείς.

Παρά το Play Protect, και το κατάστημα της Google την πάτησε πρόσφατα. Τον Σεπτέμβριο του 2019 επιβεβαιώθηκε ότι το κακόβουλο λογισμικό Joker σε 24 apps, είχε κατέβει από το Google Play περισσότερες από μισό εκατομμύριο φορές.

Ωστόσο, αυτό δεν σημαίνει πως όσοι εγκαθιστούν εφαρμογές αποκλειστικά από το Google Play είναι απόλυτα ασφαλείς.

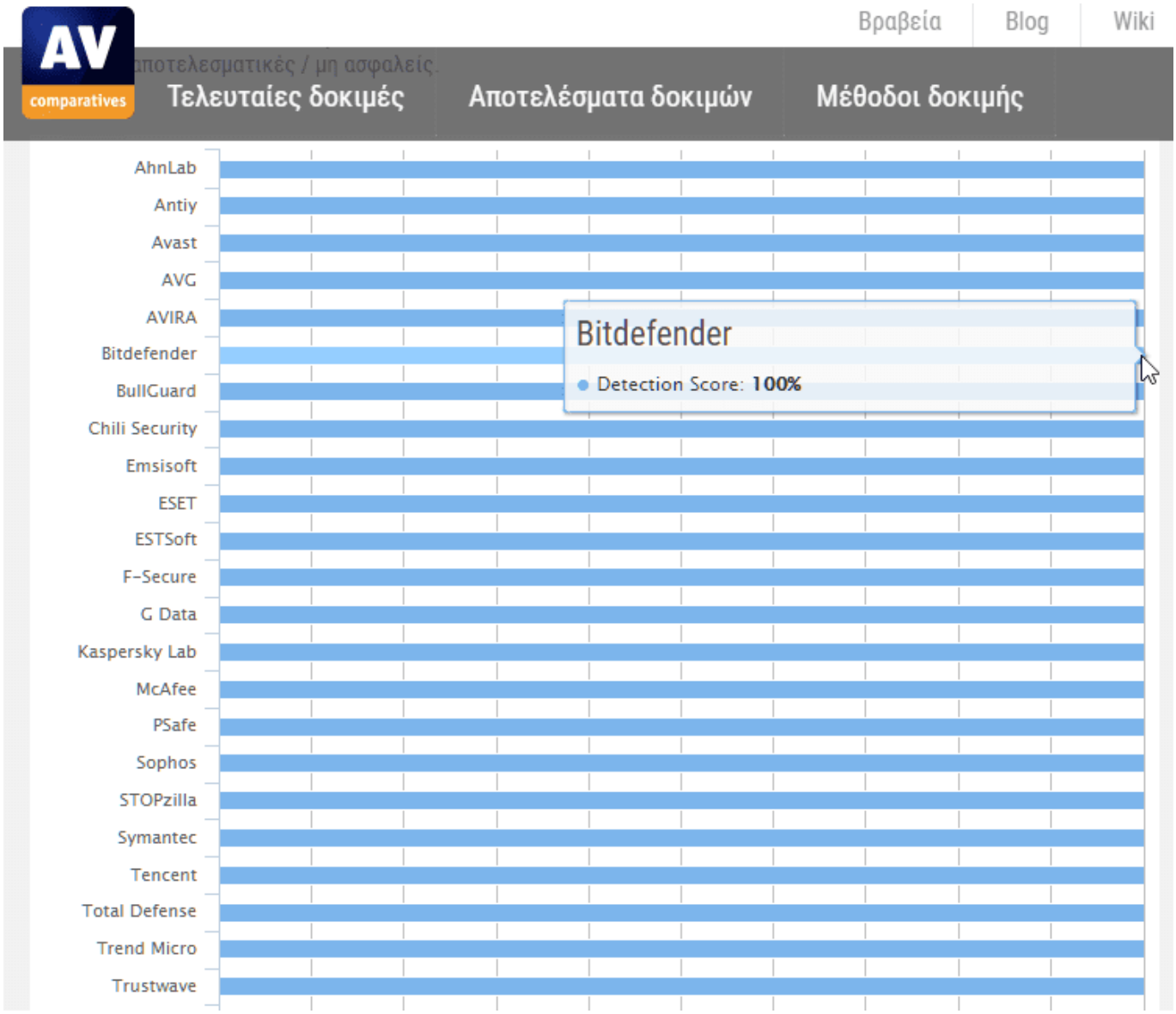
Παρά το Play Protect, και το κατάστημα της Google την πάτησε πρόσφατα. Τον Σεπτέμβριο του 2019 επιβεβαιώθηκε ότι το κακόβουλο λογισμικό Joker σε 24 apps, είχε κατέβει από το Google Play περισσότερες από μισό εκατομμύριο φορές.

Επίσης, ο ιός στο Android μπορεί να περιλαμβάνει πιο ήπιες απειλές, τις οποίες δεν τις αναγνωρίζουν τα περισσότερα δωρεάν antivirus. Για παράδειγμα, εφαρμογές που εμφανίζουν πολλές διαφημίσεις και συλλέγουν αθόρυβα προσωπικές μας πληροφορίες.

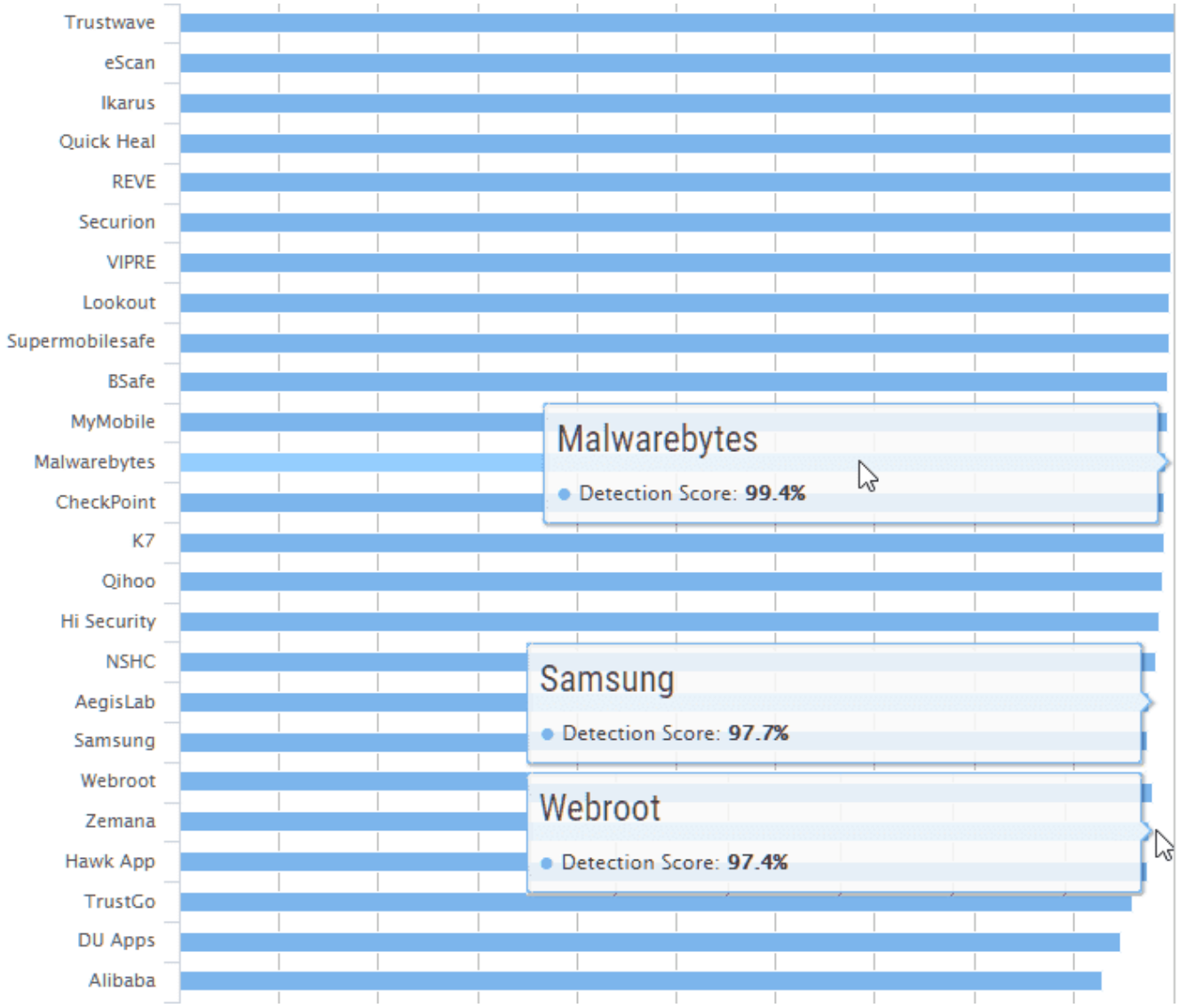
Οι μοναδικές εφαρμογές που είχαν 100% επιτυχία στην έγκαιρη ανίχνευση κακόβουλου λογισμικού κάθε μορφής, αλλά και επιτυχή αφαίρεση ιών από κινητό, ήταν 23 πληρωμένες εφαρμογές στο Android.

Πρόκειται για πλήρεις σουίτες γνωστών εταιρειών. Ελέγχουν σε βάθος τις εγκατεστημένες εφαρμογές για πιθανά προβλήματα απορρήτου, και διαθέτουν προστασία πολλαπλών επιπέδων για Ransomware.

Είναι αυτές που βλέπουμε σε αλφαβητική σειρά στον παρακάτω επίσημο πίνακα που δημοσίευσε το AV-Comparatives.



Στα τεστ απέτυχαν ακόμη και παραδοσιακά app αντιμετώπισης του malware, καθώς επίσης και ενσωματωμένα εργαλεία των κατασκευαστών. Όπως παρατηρούμε, κάποια είχαν μικρότερο ποσοστό αποτυχίας, και κάποια άλλα μεγαλύτερο.



Ως εκ τούτου, γίνεται εύκολα αντιληπτό ότι είμαστε ιδιαίτερα εκτεθειμένοι σε τέτοιους ιούς του Android.

Ιδίως αν δεν είχαμε προβλέψει ευθύς εξαρχής να τρέχουμε κάποιο πληρωμένο πρόγραμμα προστασίας από κακόβουλο λογισμικό, ή έστω ένα ισχυρό δωρεάν antivirus όπως το βραβευμένο Bitdefender.

Αξίζει να σημειώσουμε πως η πλήρης σουίτα Bitdefender Mobile Security παρέχεται δωρεάν μαζί με το Bitdefender Total Security Multi Device, καθώς και το Bitdefender Family Pack για τα PC.

Τα συμπτώματα του malware στο Android

Ο ιός στο Android τείνει να λειτουργεί αόρατος στο παρασκήνιο για να αποφύγει τη γρήγορη αναγνώριση που θα οδηγήσει στην έγκαιρη αφαίρεση του. Συνήθως, εκτελεί επαναλαμβανόμενες εργασίες που χρησιμοποιούν τους πόρους της συσκευής μας.

Παρ’ όλα αυτά, είμαστε σε θέση να ανιχνεύσουμε την παρουσία του, έστω και καθυστερημένα. Τα σημάδια ενός malware που τρέχει στο παρασκήνιο ποικίλουν. Συνήθως, εμφανίζονται με τους ακόλουθους τρόπους:

Το κινητό μας, παρότι καινούργιο, λειτουργεί πιο αργά από ό,τι θα περιμέναμε.
Η διάρκεια ζωής της μπαταρίας φαίνεται να είναι δραματικά μικρότερη από το συνηθισμένο.
Εμφάνιση αγνώστων εφαρμογών που δεν θυμόμαστε να τις έχουμε εγκαταστήσει.
Εμφανίζονται πολλές αναδυόμενες διαφημίσεις.
Οι εφαρμογές μας δεν ανοίγουν το ίδιο γρήγορα όπως είχαμε συνηθίσει.
Ανεξήγητη χρήση δεδομένων κινητής τηλεφωνίας.
Αύξηση λογαριασμών τηλεφώνου.

Πώς κάνω αφαίρεση ιών από κινητό

Όπως αναφέραμε, η πιο απλή και γρήγορη μέθοδος για αφαίρεση ιού από κινητό είναι η επαναφορά εργοστασιακών ρυθμίσεων.

Όπως όμως και το format στον υπολογιστή, το factory reset θα διαγράψει όλα τα δεδομένα στο κινητό μας. Εφαρμογές, ρυθμίσεις, και όλες τις φωτογραφίες και τα βίντεο που έχουμε τραβήξει, και είναι ενδεχομένως αναντικατάστατα.

Τα καλά νέα είναι πως υπάρχουν και άλλες λύσεις για την αφαίρεση ιών από κινητό. Η εργοστασιακή επαναφορά πρέπει να είναι η τελευταία μας επιλογή.

Παρ’ όλα αυτά, είμαστε σε θέση να ανιχνεύσουμε την παρουσία του, έστω και καθυστερημένα. Τα σημάδια ενός malware που τρέχει στο παρασκήνιο ποικίλουν. Συνήθως, εμφανίζονται με τους ακόλουθους τρόπους:

Το κινητό μας, παρότι καινούργιο, λειτουργεί πιο αργά από ό,τι θα περιμέναμε.
Η διάρκεια ζωής της μπαταρίας φαίνεται να είναι δραματικά μικρότερη από το συνηθισμένο.
Εμφάνιση αγνώστων εφαρμογών που δεν θυμόμαστε να τις έχουμε εγκαταστήσει.
Εμφανίζονται πολλές αναδυόμενες διαφημίσεις.
Οι εφαρμογές μας δεν ανοίγουν το ίδιο γρήγορα όπως είχαμε συνηθίσει.
Ανεξήγητη χρήση δεδομένων κινητής τηλεφωνίας.
Αύξηση λογαριασμών τηλεφώνου.

Πώς κάνω αφαίρεση ιών από κινητό
Όπως αναφέραμε, η πιο απλή και γρήγορη μέθοδος για αφαίρεση ιού από κινητό είναι η επαναφορά εργοστασιακών ρυθμίσεων.

Όπως όμως και το format στον υπολογιστή, το factory reset θα διαγράψει όλα τα δεδομένα στο κινητό μας. Εφαρμογές, ρυθμίσεις, και όλες τις φωτογραφίες και τα βίντεο που έχουμε τραβήξει, και είναι ενδεχομένως αναντικατάστατα.

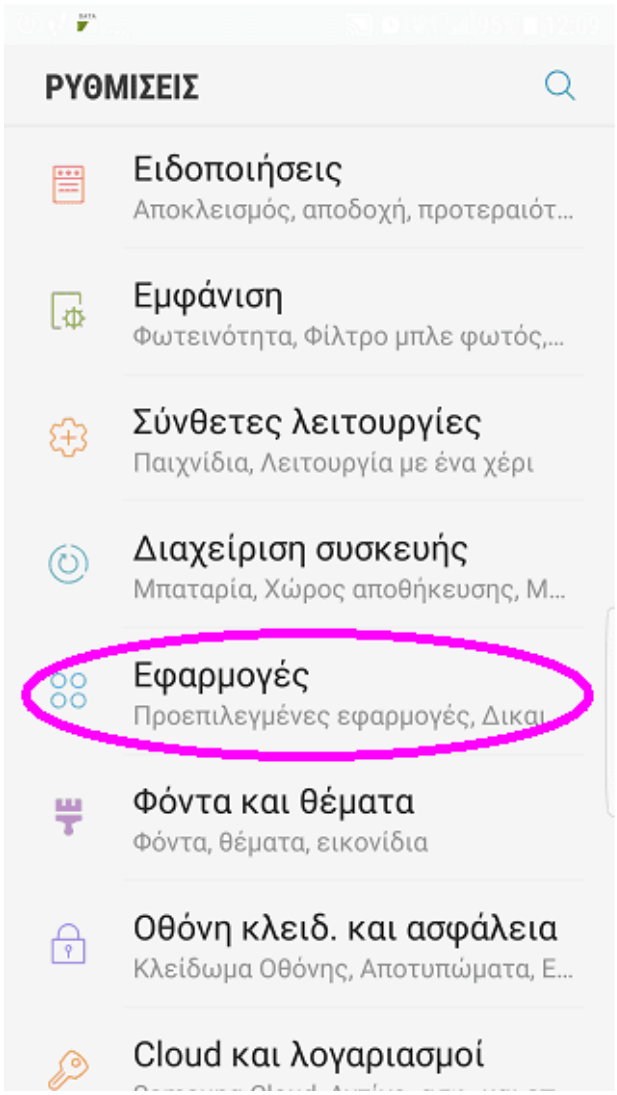
Τα καλά νέα είναι πως υπάρχουν και άλλες λύσεις για την αφαίρεση ιών από κινητό. Η εργοστασιακή επαναφορά πρέπει να είναι η τελευταία μας επιλογή.

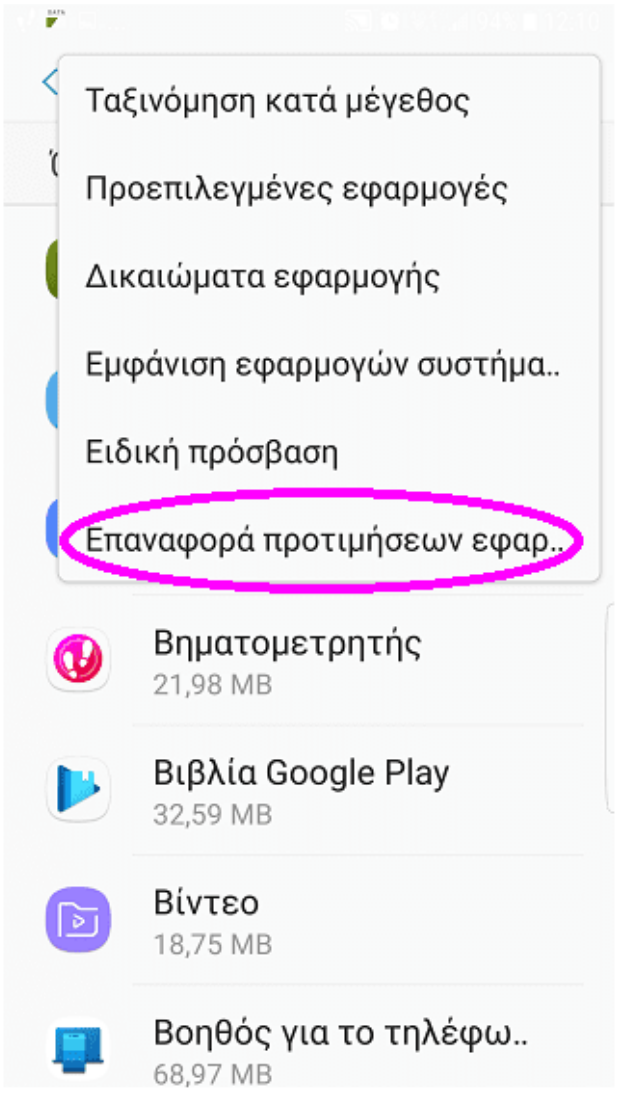
Παρ’ όλα αυτά, είμαστε σε θέση να ανιχνεύσουμε την παρουσία του, έστω και καθυστερημένα. Τα σημάδια ενός malware που τρέχει στο παρασκήνιο ποικίλουν. Συνήθως, εμφανίζονται με τους ακόλουθους τρόπους:

Το κινητό μας, παρότι καινούργιο, λειτουργεί πιο αργά από ό,τι θα περιμέναμε.
Η διάρκεια ζωής της μπαταρίας φαίνεται να είναι δραματικά μικρότερη από το συνηθισμένο.
Εμφάνιση αγνώστων εφαρμογών που δεν θυμόμαστε να τις έχουμε εγκαταστήσει.
Εμφανίζονται πολλές αναδυόμενες διαφημίσεις.
Οι εφαρμογές μας δεν ανοίγουν το ίδιο γρήγορα όπως είχαμε συνηθίσει.
Ανεξήγητη χρήση δεδομένων κινητής τηλεφωνίας.
Αύξηση λογαριασμών τηλεφώνου.
Πώς κάνω αφαίρεση ιών από κινητό
Όπως αναφέραμε, η πιο απλή και γρήγορη μέθοδος για αφαίρεση ιού από κινητό είναι η επαναφορά εργοστασιακών ρυθμίσεων.

Όπως όμως και το format στον υπολογιστή, το factory reset θα διαγράψει όλα τα δεδομένα στο κινητό μας. Εφαρμογές, ρυθμίσεις, και όλες τις φωτογραφίες και τα βίντεο που έχουμε τραβήξει, και είναι ενδεχομένως αναντικατάστατα.

Τα καλά νέα είναι πως υπάρχουν και άλλες λύσεις για την αφαίρεση ιών από κινητό. Η εργοστασιακή επαναφορά πρέπει να είναι η τελευταία μας επιλογή.

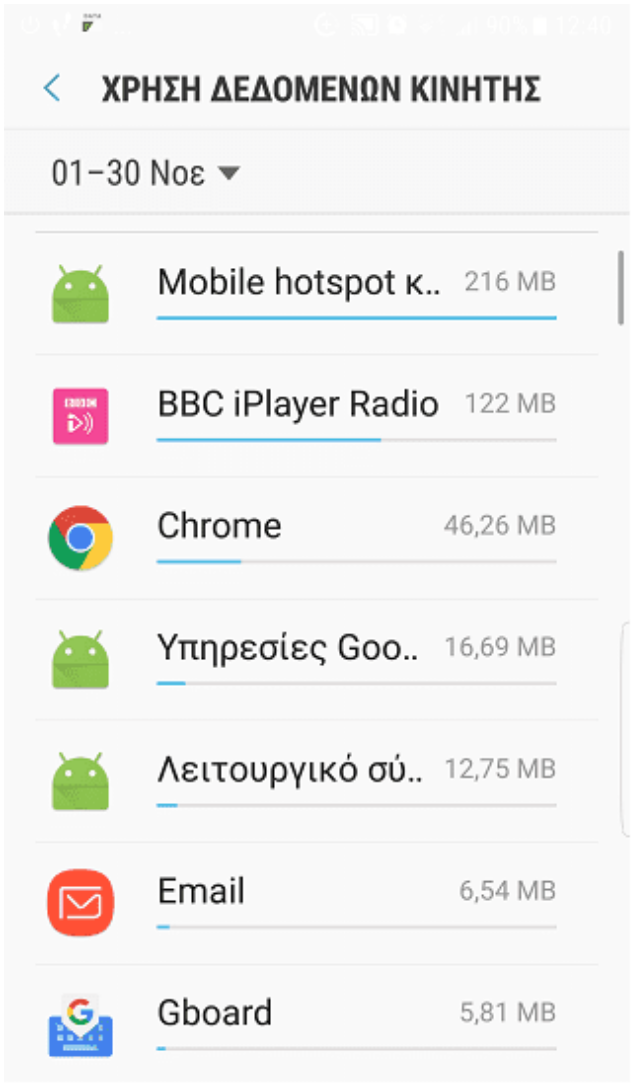


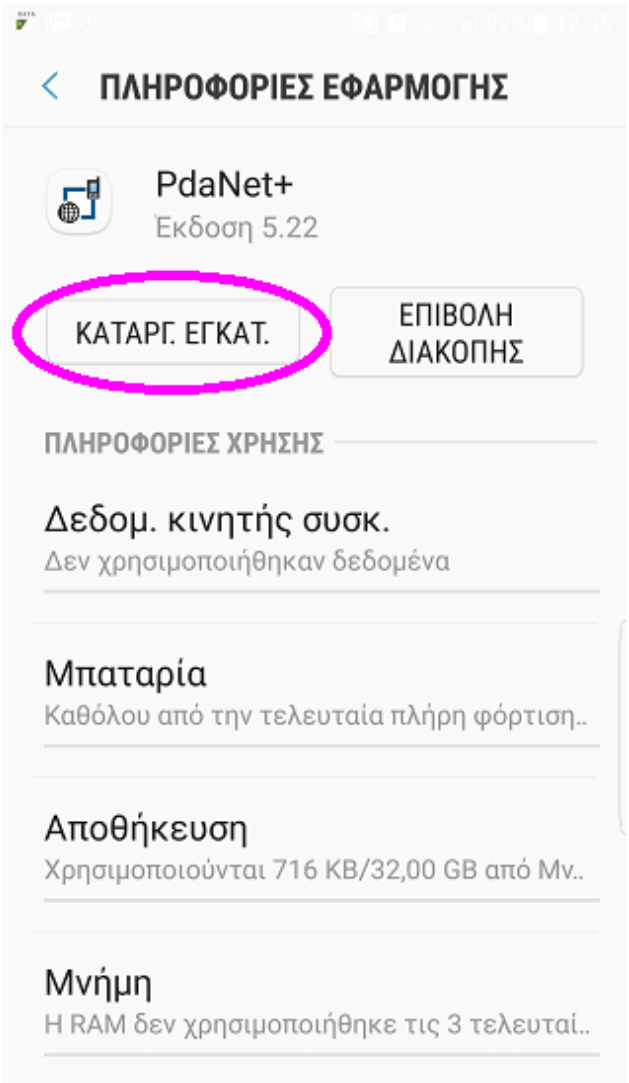


Στη συνέχεια, αναζητούμε προσεκτικά τυχόν εφαρμογές που δεν ανήκουν στο σύστημα, τις οποίες δεν θυμόμαστε να έχουμε εγκαταστήσει και δεν γνωρίζουμε. Εφόσον εντοπίσουμε τέτοια app, τα καταργούμε αμέσως από την συσκευή μας.

Κατόπιν, μέσα από τις ρυθμίσεις πηγαίνουμε στο μενού της χρήσης δεδομένων κινητής, αλλά και της μπαταρίας.

Παρατηρούμε αν υπάρχει κάποιο app που δεν το γνωρίζουμε, το οποίο καταναλώνει υπερβολικά πολλούς πόρους. Αν εντοπίσουμε κάτι τέτοιο, το καταργούμε και αυτό.





Ασφαλής λειτουργία

Υπάρχουν περιπτώσεις που το κακόβουλο λογισμικό είναι επίμονο και τόσο καλά κρυμμένο που δεν εντοπίζεται εύκολα, ή δεν επιτρέπει την κατάργηση του app στο οποίο τρέχει.

Έτσι, αν οι παραπάνω ενέργειες δεν μας έλυσαν τα προβλήματα δυσλειτουργίας στην συσκευή μας και θεωρούμε ότι το malware δεν έχει απομακρυνθεί, προχωράμε στην αφαίρεση ιού από κινητό μέσα από την ασφαλή λειτουργία.

Το safe mode θα εκκινήσει τη συσκευή μας σε ένα ασφαλές περιβάλλον μόνο με το λογισμικό που διέθετε αρχικά.

Η ασφαλής λειτουργία είναι χρήσιμη και σε περίπτωση που ορισμένες εφαρμογές που κατεβάσαμε κάνουν τη συσκευή μας να επανεκκινεί συνεχώς, να παγώνει, ή να παρουσιάζει σφάλματα και καθυστερήσεις.

Επανεκκίνηση σε ασφαλή λειτουργία

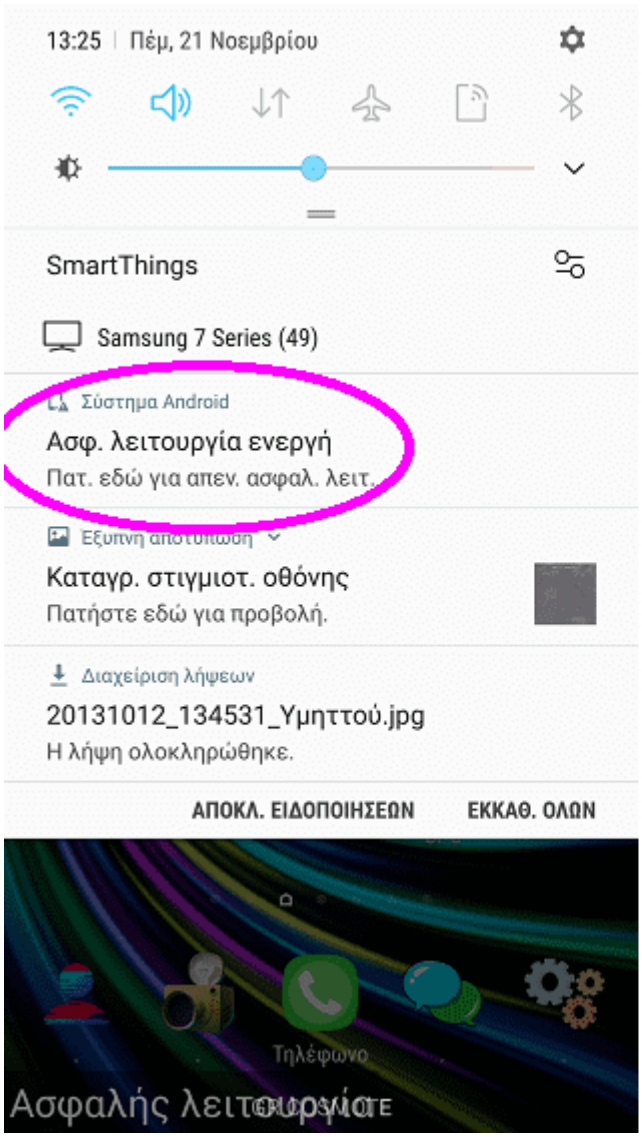
Εάν η συσκευή μας είναι ενεργοποιημένη, για να εισέλθουμε σε safe mode σε κάποια κινητά αρκεί να πιέσουμε παρατεταμένα το κουμπί λειτουργίας (power). Έπειτα, στην οθόνη αγγίζουμε παρατεταμένα το εικονίδιο απενεργοποίησης.

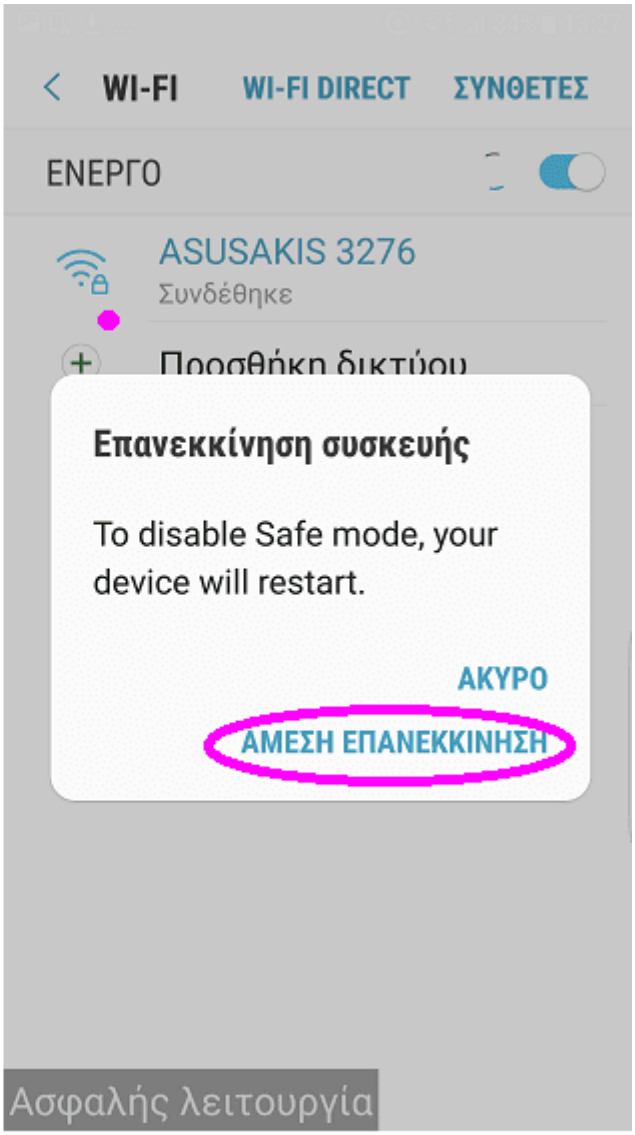
Στη συνέχεια, στο κάτω μέρος της οθόνης θα εμφανιστεί η σχετική ένδειξη. Εδώ πρέπει να σημειώσουμε ότι η διαδικασία με τα πλήκτρα για να ενεργοποιήσουμε την ασφαλή λειτουργία μπορεί να διαφέρει ανάλογα με τη συσκευή.

Συνήθως, στα περισσότερα κινητά το safe mode υλοποιείται πιο εύκολα με την επανεκκίνηση. Όταν ξεκινήσει η κινούμενη εικόνα με το λογότυπο της εταιρείας, πατάμε παρατεταμένα το κουμπί μείωσης της έντασης ήχου της συσκευής. Απλά το κρατάμε πατημένο μέχρι να ολοκληρωθεί η προβολή του.

Από εδώ και μετά, η συσκευή μας είναι παντελώς καθαρή. Τρέχει σε ένα ασφαλές περιβάλλον μόνο με το λογισμικό που διέθετε αρχικά, και μπορούμε να καταργήσουμε τις εφαρμογές που εντοπίσαμε με τις προηγούμενες μεθόδους.

Μόλις τελειώσουμε την εκκαθάριση, απλά από το επάνω μέρος της οθόνης πρέπει να σύρουμε προς τα κάτω για να εμφανιστούν οι ειδοποιήσεις. Κατόπιν, πατάμε τις σχετικές ενδείξεις που παρατηρούμε παρακάτω, έτσι ώστε να εξέλθουμε από την ασφαλή λειτουργία.





Πηγή: **pcsteps.gr**