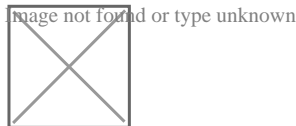


19 Μαρτίου 2016

# Subgraph OS: Ασφαλές, δωρεάν, Open Source Linux OS για όλους!

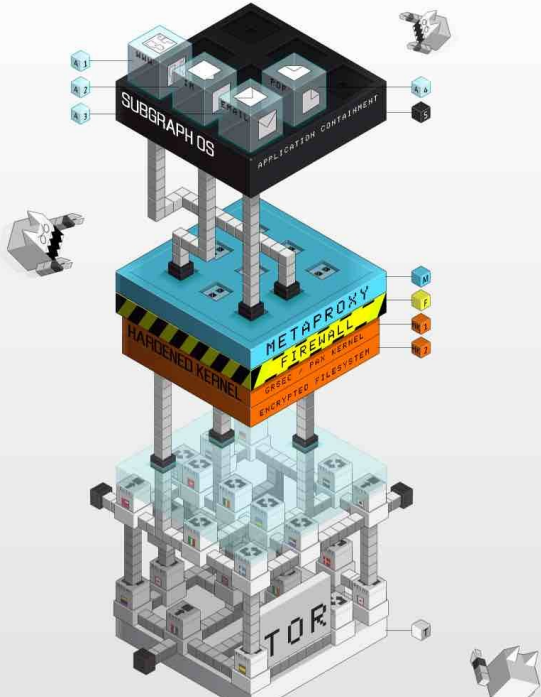
/ [Πεμπτούσια](#)



**Εν συντομία: Για να απαντήσουμε στις ανησυχίες που σχετίζονται με την ασφάλεια, το Subgraph OS είναι εδώ ως ένα ελεύθερο, ασφαλές, ανοικτού κώδικα λειτουργικό σύστημα Linux για τους χρήστες που δεν σχετίζονται με την τεχνολογία. Αυτή η διανομή που εστιάζει στην ασφάλεια έρχεται με πλήρη ενσωμάτωση του TOR, πλήρη κρυπτογράφηση δίσκου, ενσωμάτωση OpenPGP ταχυδρομείου, system hardening και άλλα τέτοια χαρακτηριστικά. Μάθετε περισσότερα για το λειτουργικό σύστημα και να κάντε το σύστημά σας ασφαλές.**

Τον τελευταίο καιρό, έχουμε δει μια αύξηση του αριθμού των υπηρεσιών ανταλλαγής μηνυμάτων και e-mail που παρέχουν μια ασφαλή επικοινωνία με τους άλλους. Για τη διασφάλιση ότι η χρήση του [internet](#) παραμένει ανώνυμη, έχουμε εργαλεία όπως το TOR software suite και οι υπηρεσίες VPN. Αλλά, τι γίνεται με την ασφάλεια των συνολικών συστημάτων; Για να απαντήσουμε στο ερώτημα αυτό,

μια εταιρεία από τον Καναδά που ονομάζεται Subgraph επικεντρώνεται στην διανομή του Linux που ονομάζεται Subgraph OS. Το λειτουργικό σύστημα έχει ως στόχο να αντιστέκεται στις hacking επιθέσεις πιο εύκολα από ότι τα κοινά χρησιμοποιούμενα μηχανήματα και τα καθημερινά [laptops](#). Αυτό το ελεύθερο και ανοικτού κώδικα λειτουργικό σύστημα έχει σχεδιαστεί από το μηδέν για να μειωθούν οι κίνδυνοι παρεμβολών και κίνδυνοι παρακολούθησης που μπορεί να υπάρχουν στα τερματικά.

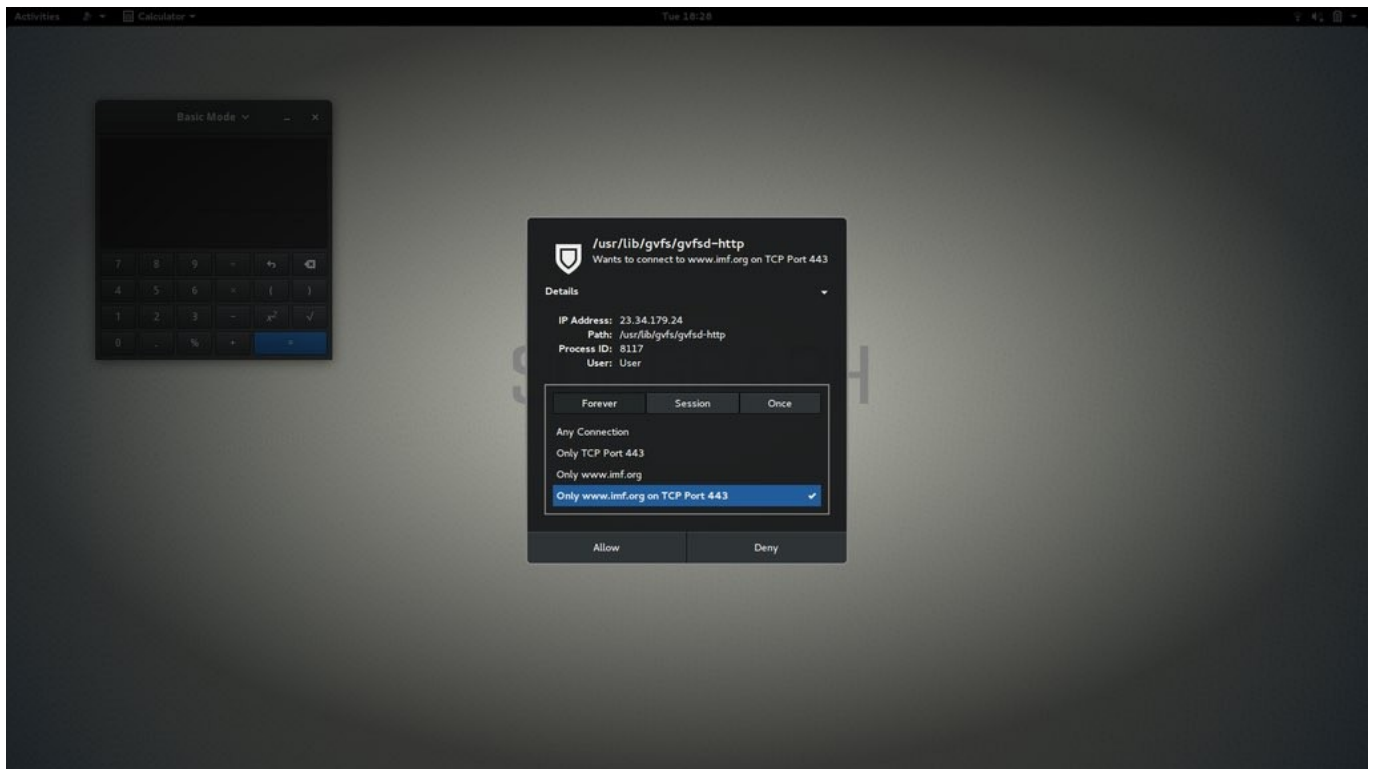


### SUBGRAPH OS

- Using LXC (Linux Containers) and Xpra, commonly used applications are completely separated from the main operating system. Our application containers are configured to isolate the application from the file system, prevent keyloggers from sniffing keystrokes from other X11-based applications, and block network access by applications that do not require it. All of this runs inside a Grsecurity-enabled kernel to make it much more difficult for compromised applications to escape their containers.
- Subgraph OS is packaged with the Tor Browser (from the Tor Browser Bundle), a version of Firefox specifically configured for preserving anonymity. The Tor Browser runs in its own application container.
- Instant messaging presents challenges to security and privacy because clients are implemented in unsafe languages and end-to-end encryption is often not the default. To help address this problem in Subgraph OS, the instant messaging client runs in an application container and conducts all communications over the Tor network. Our eventual goal is to implement our own instant messaging client in a memory-safe language, using GTR by default, and integrating with our Nymrs identity service.
- Subgraph Mail in collaboration with the Nymrs identity service makes PGP key management and sending/receiving of encrypted email easy for everybody. Subgraph Mail is also secure – implemented in a memory-safe language and internally architected so that even if parts of the application are compromised an attacker still wouldn't have access to the rest of your mail or encryption keys.
- Vulnerabilities in PDF readers compromise a lot of computers. To combat this threat, Subgraph OS isolates the PDF reader in an application container with no network access. This limits the potential of malicious PDFs to access files on the computer or initiate connections on the behalf of the attacker.
- Not every application knows how to communicate through Tor and some applications need to be specially configured. To make it easier for our users, the Subgraph Metaproxy transparently relays outgoing connections through Tor without having to configure proxy settings for each application. Connections can be relayed by application and destination. Metaproxy also makes each application connect through different circuit on the Tor network.
- The Subgraph OS application firewall allows a user to control which applications can initiate outgoing connections. When an unknown application attempts to make an outgoing connection, the user will be prompted to allow or deny the connection on a temporary or permanent basis. This helps prevent malicious applications from phoning home.
- Subgraph OS comes with a Grsecurity-enabled kernel by default. Grsecurity features such as PaX complicate exploitation of security vulnerabilities such as buffer overflows in applications and the operating system kernel.
- Subgraph OS installer requires the user to use full disk encryption with Linux's trusted dm-crypt/LUKS mechanism. Additionally, the system's memory is wiped on shutdown to help mitigate cold boot attacks designed to steal your encryption keys.
- By default, Subgraph OS only communicates through the Tor network. Anonymous web browsing is done using the Tor browser, and other applications are transparently forced through Tor. This means that all outgoing connections are anonymous. If the user needs to browse the web non-anonymously then we also provide a non-anonymous browser that is contained from the rest of the operating system.

Με έμφαση στην ασφάλεια, το Subgraph OS έχει σχεδιαστεί για να «σκληρύνει» το σύστημα και να το να κάνει να προλαμβάνει τους κινδύνους. Το λειτουργικό σύστημα δίνει, επίσης, έμφαση στην ακεραιότητα της εγκατάστασης [πακέτων λογισμικού](#). Εκτός από την παροχή ασφάλειας του πυρήνα, το Subgraph OS διαθέτει πλήρη κρυπτογράφηση δίσκου και έναν τρόπο για να ανοίγει σε ένα περιβάλλον δοκιμών ([sandbox](#)) τις απειλές για να μειώσει την έκθεση του χρήστη.

Με την ενσωμάτωση του OpenPGP ταχυδρομείου, οι χρήστες έχουν πρόσβαση σε υπογεγραμμένο κρυπτογραφημένο μήνυμα ηλεκτρονικού ταχυδρομείου. Τα πάντα έχουν σχεδιαστεί με μια «εύκολη» προσέγγιση, έτσι ώστε δεν θα υπάρξει ανάγκη για να εκτελεστούν εντολές σε ένα τερματικό παράθυρο ή σε οποιαδήποτε εξωτερικό [plug-in](#).



Η [TOR](#) ανωνυμία ρυθμίζει όλη η κυκλοφορία του χρήστη μέσα από αυτό, καθιστώντας δυσκολότερο στον εισβολέα να καταλάβει τη φυσική θέση των στόχων του. Ωστόσο, το έργο επικεντρώνεται περισσότερο στην ασφάλεια από ότι στην ανωνυμία. Καθώς το λειτουργικό σύστημα χρησιμοποιεί την εφαρμογή Metaroxy για να προσδιορίσει τη μετάδοση προς τον έξω κόσμο, μπορείτε να αναγνωρίσετε εύκολα τις νόμιμες συνδέσεις.

Η τρέχουσα έκδοση του Subgraph OS είναι στο pre-alpha στάδιο. Μπορείτε να μάθετε περισσότερα για το Subgraph OS στην [ιστοσελίδα](#) του και στο [GitHub repository](#).

Πηγή: [secnews.gr](#)